**UNITED STATES DISTRICT COURT**
**DISTRICT OF NEW JERSEY**

| | |
|---|---|
| IN RE: SAMSUNG CUSTOMER DATA SECURITY BREACH LITIGATION | Civil Action No. 1:23-md-03055 (CPO-EAP) |
| | (MDL 3055) |
| *This Document Relates To:* ALL ACTIONS | District Judge Christine P. O'Hearn<br>Magistrate Judge Elizabeth A. Pascal |

# DEFENDANT SAMSUNG ELECTRONICS AMERICA, INC.'S BRIEF IN SUPPORT OF MOTION TO DISMISS AMENDED CONSOLIDATED COMPLAINT

**ARCHER & GREINER, P.C.**
1025 Laurel Oak Road
Voorhees, NJ 08043
T: (856) 795-2121 / F: (856) 795-0574

**HUNTON ANDREWS KURTH LLP**
2200 Pennsylvania Ave. NW
Washington, DC 20009
T: (202) 955-1500 / F: (202) 778-2201

**ARNOLD & PORTER KAYE SCHOLER LLP**
250 West 55th Street
New York, NY 10019
T: (212) 836-8000 / F: (212) 836-8689

*Attorneys for Defendant*
*Samsung Electronics America, Inc.*

# TABLE OF CONTENTS

**Page**

# TABLE OF AUTHORITIES

**Page(s)**

## Federal Cases

**State Cases**



*Champion ex rel. Ezzo v. Dunfee*,
939 A.2d 825 (N.J. Super. Ct. App. Div. 2008) .....40, 42

**Federal Statutes**



**State Statutes**

**Rules**



**Other Authorities**

Defendant Samsung Electronics America, Inc. ("Samsung") moves to dismiss Plaintiffs' Consolidated Amended Complaint ("Complaint") in its entirety with prejudice pursuant to Fed. R. Civ. P. 12(b)(6). Samsung also submits, for the Court's convenience, Appendices detailing the numerous reasons why each of the individual named Plaintiffs' claims fail.

## INTRODUCTION

In late July 2022, Samsung was the victim of a criminal attack that involved customer information (the "Security Incident"). The Security Incident, however, ***did not*** involve the personal information often involved in data breach cases, such as driver's license numbers, bank account, credit or debit card numbers, Social Security numbers, tax identification numbers, passports, voice recordings, health information, or biometrics. Instead, the Security Incident was limited to name, contact and demographic information, date of birth, and product registration information. Despite having no legal obligation to notify its customers outside of North Dakota and Washington,[1] Samsung proactively and directly notified ***all*** potentially affected United States customers via e-mail and by posting a Notice on

[1] North Dakota and Washington require customer notification if the data elements include first name with last name along with date of birth. Other states require data elements such as Social Security numbers, debit or credit card information in combination with linked security or access code, or health information.

(Footnote Cont'd on Following Page)

its website.[2]

Samsung's Notice assured its customers "that the issue did not impact Social Security numbers or credit and debit card numbers, but in some cases, may have affected information such as name, contact and demographic information, date of birth, and product registration information." *Id.* Remarkably, within ***two hours*** of providing its Notice, the first of 17 class action lawsuits was filed. The others were filed shortly thereafter. After consolidation by the Judicial Panel on Multidistrict Litigation, Samsung now faces a 279-page Complaint that includes the varied claims of 49 individual Plaintiffs from 34 states alleging more than 50 different state common law and statutory causes of action.

Despite the hundreds of pages, the Complaint pleads very few actual factual allegations. Even a cursory review of the Complaint quickly reveals that this lawsuit is propped up by pure speculation about "injuries" that could not possibly have been caused by the Security Incident. For example:

- Plaintiff Erica Fletcher alleges that, at an unspecified time after July 2022, she suffered injury in the form of the "***misuse of her PII on***

[2] *See* Declaration of Neil Gilman ("Gilman Decl.") at Ex. A, *Important Notice Regarding Customer Information*, Sept. 2, 2022, ("Notice") *available at* https://www.samsung.com/us/support/securityresponsecenter/. Plaintiffs incorporate this Notice explicitly into their pleading. (Am. Compl. ¶ 211.)

***Instagram***." (Am. Compl. ¶ 34 (emphasis added).)

- Plaintiff Matthew McIntyre alleges that, at an unspecified time after July 2022, he suffered injury in the form "of ***a fraudulent loan*** taken out in his name, ***fraudulent charges on his debit card*** amounting to over $600, and ***over 120 credit inquiries*** under his name." (*Id.* ¶ 67 (emphasis added).)
- Plaintiff Darren Glean alleges that, at an unspecified time after July 2022, he suffered injury in the form of "***unauthorized charges on his credit cards***" the result of which he has spent "***nearly 100 hours***" addressing. (*Id.* ¶ 70 (emphasis added).)
- Plaintiff Harold Nyanjom alleges that, at an unspecified time after July 2022, he suffered "***unauthorized charges on his AT&T account***." (*Id.* ¶ 94 (emphasis added).)
- Plaintiff Peggy Rodriguez alleges that, at an unspecified time after July 2022, she suffered "***an unauthorized charge on her Comcast Xfinity account***" and two alleged "***fraudulent charges on her debit card*** in the amounts of $135 and $200 purportedly ***from Michigan Lottery***." (*Id.* ¶ 88 (emphasis added).)
- Plaintiff Tonisha Jordan alleges that, at an unspecified time after July

2022, she suffered "fraud in the form of ***unauthorized charges on her Paypal account***." (*Id.* ¶ 139 (emphasis added).)

The Complaint contains ***no*** facts explaining how it is plausible that any of these alleged injuries were caused by the Security Incident. Rather, the only "fact" pled in the Complaint is that these alleged injuries occurred at some unspecified point after July 2022. Such injuries are wholly implausible as none of these Plaintiffs allege that they provided Samsung their Instagram password, their AT&T or Xfinity account information, their PayPal account information, credit or debit card number, or a Social Security number when purchasing a Samsung device, registering that device with Samsung, or creating a Samsung account. In fact, ***none*** of the 49 Plaintiffs actually allege they registered any device with Samsung, purchased any device directly from Samsung, or even created a Samsung account.

Plaintiffs clearly recognized the impossibility of these disparate alleged injuries being caused by the exposure of the information identified in Samsung's Notice. To avoid this dispositive problem, Plaintiffs ignore Samsung's Notice, despite relying on this document throughout their Complaint, and allege that Social Security numbers and credit or debit card numbers ***were*** implicated in the Security

Incident.[3] (Am. Compl. ¶ 26.) Plaintiffs provide no basis for this allegation and, in fact, there is none, which Plaintiffs effectively admit by making the allegation solely on "information and belief."

Based on these fatally flawed and cursory allegations, Plaintiffs assert 61 counts in total: 7 common law counts (negligence, negligence *per se*, breach of contract, breach of implied contract, breach of confidence, unjust enrichment and declaratory judgment), and 54 state statutory counts. Plaintiffs' claims all fail.

- Plaintiffs' claims all require cognizable injury or damages. The disparate "injuries" alleged by Plaintiffs are the very types of alleged harms that often result in dismissals for lack of injury and damages.
- Plaintiffs' negligence claims are barred by the economic loss doctrine and, regardless, Plaintiffs fail to establish that Samsung owed them a duty or plead facts sufficient to allege Samsung breached any purported duty to provide reasonable data security.
- Plaintiffs' negligence *per se* claims are not a separate cause of action in many states and, even where the claims are recognized, they fail because Plaintiffs predicate it on a federal statute that does not

[3] Even these items of personal information could not explain many of the injuries alleged by Plaintiffs, such as the access to the PayPal or Xfinity accounts.

provide a private right of action and undisclosed statutory grounds.

- Plaintiffs' breach of confidence claims are not a recognized cause of action in many states or are recognized only in limited circumstances inapplicable here and, regardless, Plaintiffs cannot allege breach of confidence for the simple reason that courts uniformly hold that a data breach does not satisfy the intentional disclosure requirement necessary to state such a claim.
- Plaintiffs' unjust enrichment claims fail because, even in states where unjust enrichment is a recognized cause of action, Plaintiffs do not allege a direct relationship with Samsung, that they conferred a benefit upon Samsung, or that there is no adequate remedy at law.
- Plaintiffs' declaratory judgment claim should be dismissed because declaratory judgment is a remedy, not a cause of action.
- Plaintiffs' host of statutory claims fail for several independent reasons, including threshold reasons such as: (1) the absence of a private right of action, (2) prohibitions or limitations on class actions, (3) Plaintiffs' utter failure to provide pre-suit notice, or (4) statutory limitations permitting only injunctive relief. In addition, Plaintiffs fail to plead their claims with the required particularity under Rule 9(b), or

sufficiently allege the elements of their claims, including reliance, proximate causation, knowledge or intent, a consumer transaction, and/or a duty to disclose any allegedly omitted information.

Plaintiffs cannot ignore the Notice, which they explicitly rely on, by alleging a laundry list of disparate injuries that could not have possibly been caused by the Security Incident and that lack any factual support or connection to the Security Incident. For these and other reasons set forth below, Samsung respectfully requests that the Court dismiss Plaintiffs' Complaint in its entirety with prejudice.

## BACKGROUND

### I. THE SECURITY INCIDENT

Samsung was the victim of a criminal attack in late July 2022, when cyber-criminals stole information from some of Samsung's U.S. systems (the "Security Incident"). (Am. Compl. ¶ 211.) Plaintiffs allege that on August 4, 2022, Samsung discovered the personal information of some of its customers was affected by the Security Incident. (*Id.* ¶ 212.) This information was limited only to "name, contact and demographic information, date of birth, and product registration information." (*Id.* ¶ 213.)

Samsung undertook a comprehensive and diligent investigation and provided notification to potentially affected customers on September 2, 2022—a

mere 29 days after Samsung discovered that the Security Incident involved personal information. (*Id.* ¶¶ 211-12.) Plaintiffs allege ***no*** facts suggesting Samsung knew or should have known about the Security Incident earlier, or that Samsung unreasonably delayed notification.

## II. SAMSUNG'S NOTICE OF THE SECURITY INCIDENT

Samsung proactively provided direct notification of the Security Incident via e-mail to all potentially affected United States customers. (*Id.* ¶ 211.) Samsung also posted its Notice regarding the Security Incident on its website along with frequently asked questions, both of which are still available on Samsung's website today and are referred to explicitly in the Complaint. (*Id.* ¶ 211.)

In the Notice, Samsung reassured its customers that the Security Incident "did not impact Social Security numbers or credit and debit card numbers," or other sensitive information necessary to commit identity theft or fraud. Gilman Decl. at Ex. A, Notice. Instead, the affected data was limited to information such as "name, contact and demographic information, date of birth, and product registration information." *Id.*; *see also* (Am. Compl. ¶ 211, referring to the Notice). Samsung also made clear that not everyone receiving the Notice was affected by the Security Incident or affected in the same way, meaning that one person may have only had their email address impacted while others may have had

their name and date of birth impacted. *See* Gilman Decl. at Exhibit A, Notice. Samsung clarified that it was providing notice to its customers "to make them aware of this matter." *See id*.

## III. PLAINTIFFS SUE SAMSUNG WITHIN HOURS OF THE NOTICE

Within hours of Samsung's announcement, the first of 17 lawsuits was filed. After the Judicial Panel on Multidistrict Litigation consolidated the cases in this Court, Plaintiffs cobbled together 49 individual Plaintiffs from 34 states alleging the violation of nearly 100 different state laws based solely on the allegation that Samsung failed "to properly secure and safeguard the sensitive and confidential personally identifiable information" of Plaintiffs. (Am. Compl. ¶ 1.)[4]

## IV. PLAINTIFFS' ALLEGATIONS

The 49 named Plaintiffs allege that they purchased a wide array of Samsung devices, ranging from smartphones, tablets, laptops and smartwatches to printers, televisions, washers and dryers, refrigerators, microwaves, and even a robot vacuum. (*See*, *e.g.*, Am. Compl. ¶¶ 45, 54, 63, 174.) Even more varied are the instances where the named Plaintiffs allege they purchased these various devices, with date ranges from 20 years ago to July 2022 when the Security Incident

[4]After Samsung demonstrated to Plaintiffs through a meet and confer process that many of their counts were barred for various reasons, Plaintiffs filed an Amended Consolidated Complaint that withdrew approximately one-third of those counts.

occurred. (*See, e.g.*, *id.* ¶¶ 60, 174, 177.) Plaintiffs, however, uniformly fail to allege who they purchased these items from (i.e., Samsung or a retailer), the PII they allegedly provided to Samsung in connection with their purchases or use of the products, or any other specifics about their purchases. None allege to have read or relied upon any Samsung Privacy Policy before making these purchases. No one alleges any issues or defects with the devices themselves.

Plaintiffs allege a wide variety of "harms" all purportedly occurring after July 2022 and as a result of the Security Incident. Just by way of example:[5]

| Alleged Injury | Compl. ¶ |
|---|---|
| Erica Fletcher alleges "misuse of her PII on Instagram" along with "scam debt consolidation" and being "informed . . . that her PII is being sold by a third party." | 34 |
| Jacob Smith alleges "ten unauthorized charges on his Samsung Sofi Mastercard totaling $1,000." | 43 |
| Raffi Kelechian alleges that he suffered "a perceptible increase in scam/phishing emails, text messages, and/or phone calls" and that he was notified by Experian "that his PII was for sale on the Dark Web." | 52 |
| Jason Vandewater alleges that he "suffered fraud in connection with unauthorized charges on his credit card and debit card accounts." | 61 |
| Peggy Rodriguez alleges an "unauthorized charge on her Comcast Xfinity account" and two alleged "fraudulent charges on her debit card in the amounts of $135 and $200 purportedly from Michigan Lottery." | 88 |

[5] For the other alleged injuries *see* Appendix 1 (Alleged Harm Chart).

| | |
|---|---|
| Harold Nyanjom alleges "unauthorized charges on his AT&T account." | 94 |
| Michael Ortiz alleges that he "had to put a block on his Social Security Number and eventually had to get another Social Security card." | 133 |

Plaintiffs, however, fail to allege how these disparate harms could have been caused by the Security Incident. None of the Plaintiffs allege they specifically provided Samsung their Social Security number, Xfinity account information, credit card number, or Instagram password when purchasing a Samsung refrigerator or robot vacuum, registering that device with Samsung, or creating a Samsung account. Not a single one of the 49 Plaintiffs alleges they registered any device with Samsung, purchased any device directly from Samsung, or created a Samsung account. Instead, all 49 Plaintiffs merely allege that Samsung, "gathered" their "PII," without any explanation of how or why. (*See, e.g.*, Am. Compl. ¶ 33, which is repeated verbatim for all named Plaintiffs.)

Plaintiffs allege, on "information and belief," that Social Security numbers, credit or debit card numbers, and geolocation data were implicated in the Security Incident. (*Id.* ¶ 26.) Plaintiffs, however, fail to support this allegation with any facts, such as a specific allegation by any Plaintiff that they provided their Social Security Number to Samsung. And Plaintiffs fail to acknowledge that this allegation is directly contradicted by the very document they rely on throughout

their Complaint, Samsung's Notice, cited at ¶¶ 211, 219, 221, and 222 of the Complaint.

Plaintiffs also allege that Samsung had deficient security and "utterly failed to properly secure and upgrade its systems." (Am. Compl. ¶ 4.) In support, the Complaint includes a discussion of other "well-publicized" data breaches impacting Samsung's competitors. (*Id.*) The Complaint also includes a smattering of internet articles about other alleged "data security vulnerabilities" from May 2019 until December 2022. (*Id.* ¶¶ 3, 5, 203-210.) Plaintiffs, however, fail to allege why these cherry-picked and unverified internet articles relate in any way to the Security Incident or have any relevance at all.

## ARGUMENT

### V. STANDARD OF REVIEW

To survive dismissal, Plaintiffs must allege facts that demonstrate a "plausible" basis for relief. *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 556 (2007). "Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). Plaintiffs must plead "factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* at

678. Factual allegations that establish no "more than a sheer possibility" of liability are not sufficient. *Id*.

In evaluating a motion to dismiss, courts may consider documents and other "matters incorporated by reference or integral to the claim, items subject to judicial notice, matters of public record, orders, [and] items appearing in the record of the case." *Buck v. Hampton Twp. Sch. Dist.*, 452 F.3d 256, 260 (3d Cir. 2006) (quoting 5B Charles A. Wright & Arthur R. Miller, *Federal Practice & Procedure* § 1357 (3d ed. 2004)). Indeed, courts may examine such materials "without converting the motion to dismiss into one for summary judgment" because "the primary problem raised by looking to documents outside the complaint—lack of notice to the plaintiff—is dissipated '[w]here the plaintiff has actual notice . . . and has relied upon these documents in framing the complaint.'" *In re Burlington Coat Factory Sec. Litig.*, 114 F.3d 1410, 1426 (3d Cir. 1997) (quoting *Watterson v. Page*, 987 F.2d 1, 3-4 (1st Cir. 1993)).

Courts need not rely on bare factual allegations that are contradicted by documents attached to or referenced in the complaint. *See ALA, Inc. v. CCAIR, Inc.*, 29 F.3d 855, 859 n.8 (3d Cir. 1994) ("Where there is a disparity between a written instrument annexed to a pleading and an allegation in the pleading based thereon, the written instrument will control."); *Pickett v. Ocean-Monmouth Legal*

*Servs., Inc.*, 2012 WL 1601003, at *4 (D.N.J. May 7, 2012) (observing that courts are not required to "turn a blind eye to the facts as shown in documents . . . appropriately considered in deciding a motion to dismiss if those facts directly contradict the conclusory allegations in the complaint").

## VI. PLAINTIFFS FAIL TO STATE VIABLE CLAIMS FOR RELIEF

### A. Applicable Law

A federal court sitting in diversity determines the applicable substantive law by looking to the choice of law principles of the forum state. *Klaxon Co. v. Stentor Elec. Mfg. Co.*, 313 U.S. 487, 496-97 (1941); *Collins v. Mary Kay, Inc.*, 874 F.3d 176, 183 (3d Cir. 2017). While cases transferred by the Judicial Panel on Multidistrict Litigation may sometimes require a more complex choice of law analysis, those complexities do not exist here, where Plaintiffs have filed a single Complaint that supersedes the original underlying complaints as a matter of law.

"New Jersey courts apply the two pronged 'most significant relationship' test of the Restatement (Second) of Conflict of Laws." *Curtiss-Wright Corp. v. Rodney Hunt Co.*, 1 F. Supp. 3d 277, 283 (D.N.J. 2014) (citing *P.V. ex rel. T.V. v. Camp Jaycee*, 962 A.2d 453, 459 (N.J. 2008)). Step one requires the Court to determine whether there is an actual conflict between the law of the states with an interest in the claim. *P.V.*, 962 A.2d at 460. "That is done by examining the

substance of the potentially applicable laws to determine whether 'there is a distinction' between them." *Id*. If there is a difference, then a conflict exists. But that does not end the inquiry. If the outcomes would be the same, there is no conflict and "a court may refer interchangeably to the laws of each state in discussing the applicable law to the case." *On Air Ent. Corp. v. Nat'l Indem. Co.*, 210 F.3d 146, 149 (3d Cir. 2000).

However, if there is a conflict among the state laws at step one, step two requires courts to "determine which jurisdiction has the 'most significant relationship' to the claim." *Curtiss-Wright Corp.*, 1 F. Supp. 3d at 283 (citing *P.V.*, 962 A.2d 453). The Second Restatement of Conflict of Laws sets forth the relevant factors which should be analyzed in making the determination depending on the type of claim asserted, all of which support application of the law of Plaintiffs' home states. *See P.V.*, 962 A.2d at 458.

There is no doubt that state law varies greatly with respect to Plaintiffs' common law claims. *In re Ford Motor Co. Ignition Switch Prod. Liab. Litig.*, 174 F.R.D. 332, 348 (D.N.J. 1997) ("Since the laws of each of the fifty states vary on important issues that are relevant to plaintiffs' causes of action and defendants' defenses, the court cannot conclude that there would be no conflict in applying the law of a single jurisdiction."). As to the second prong, while Plaintiffs fail to

allege any cognizable injuries for the reasons discussed below, they nevertheless contend that they have suffered various forms of injury that occurred in their home states, such as actual identity theft, mitigation expenses, and lost time. (Am. Compl. ¶ 285.) Thus, the law of each Plaintiff's home state governs their common law claims.

### B. Plaintiffs' Claims Fail Because They Have Not Plead Sufficient Injury and Damages

All of Plaintiffs' claims require a showing of injury and damages.[6] A court must dismiss a data breach class action where the Plaintiffs fail to "adequately allege[]" damages "stem[ming] from a data breach." *Pruchnicki v. Envision Healthcare Corp.*, 439 F. Supp. 3d 1226, 1233 (D. Nev. 2020), *aff'd*, 845 F. App'x 613 (9th Cir. 2021) (dismissing data breach class action involving disclosure of personal information for lack of damages). In *Pruchnicki*, the defendant's systems were hacked by "an unidentified third party" who was able to gain access to highly sensitive PII, such as "name, date of birth, social security number, driver's license number, and unidentified 'financial information.'" *Id.* at 1229. Despite the data in that case being much more sensitive than the data here, the court rejected as "too

[6] *See* Appendix 2 (Negligence and Negligence *Per Se* Chart, Column G); Appendix 3 (Breach of Confidence Chart, Column B); Appendix 4 (Breach of Express and Implied Contract Chart, Columns B, C); Appendix 5 (Unjust Enrichment Chart, Column E); Appendix 6 (Statutory Claim Chart).

tenuous," "insufficient," or "conclusory" the plaintiff's theories of damages, several of which are asserted by Plaintiffs here, including "lost time mitigating the effects of the data breach, emotional distress, the 'imminent and certainly impending injury flowing from potential fraud and identity theft,' diminution in value of her personal and financial information, and continued risk to her personal date." *Id.* at 1232-36. The Ninth Circuit affirmed. *Pruchnicki v. Envision Healthcare Corp.*, 845 F. App'x 613 (9th Cir. 2021).

That injury and damages are required in data breach actions is not a new or novel proposition. The Third Circuit has dismissed claims on standing grounds, finding that there is no alleged injury where Plaintiffs failed to allege that the stolen data was misused or of the type that could be used to perpetrate identity theft. *See Reilly v. Ceridian Corp.*, 664 F.3d 38, 45 (3d Cir. 2011) ("In data breach cases where no misuse is alleged . . . there has been no injury—indeed no change in the status quo."); *Clemens v. ExecuPharm Inc.*, 48 F.4th 146, 152, 157-59 (3d Cir. 2022) (noting that "the type of data involved in a data breach may be such that mere access and publication do not cause inherent harm to the victim" but that certain data, including "social security numbers . . . taxpayer identification numbers, banking information, credit card numbers, driver's license numbers, sensitive tax forms, and passport numbers," could "be used to perpetrate identity

theft or fraud"). Given these cases, Plaintiffs' claims cannot survive the higher burden of demonstrating actual injury or damages.[7]

Other jurisdictions similarly dismissed data breach cases for failure to allege damages. Indeed, federal courts in New York, California, Nevada and other jurisdictions have all dismissed data breach class actions based on the plaintiff's "fail[ure] to adequately allege damages stemming from a data breach of [defendant] by third parties."[8] And while there are certainly data breach cases

---

[7] Courts generally recognize that the bar for plaintiffs to show an injury for standing purposes is lower than the bar for showing cognizable injury. *See In re Horizon Healthcare Servs. Inc. Data Breach Litig.*, 846 F.3d 625, 633 n.9 (3d Cir. 2017) ("[O]ur decision regarding Article III standing does not resolve whether Plaintiffs have suffered compensable damages. Some injuries may be 'enough to open the courthouse door' even though they ultimately are not compensable.'" (quoting *Doe v. Chao*, 540 U.S. 614, 625 (2004))); *Brooks Grp. & Assocs., Inc. v. LeVigne*, 2014 WL 1490529, at *8 n.48 (E.D. Pa. Apr. 15, 2014) ("'Actual damages' means something more than harm that 'satisfies the injury-in-fact and causation requirements of Article III standing.'" (quoting *Chao*, 540 U.S. at 624)).

[8] *Pruchnicki*, 845 F. App'x at 614; *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629, 639 (7th Cir. 2007) (collecting cases; holding, "[w]ithout more than allegations of increased risk of future identity theft, the plaintiffs have not suffered a harm that the law is prepared to remedy"); *Hammond v. The Bank of New York Mellon Corp.*, 2010 WL 2643307, at *2 (S.D.N.Y. June 25, 2010) (collecting cases; dismissing action "because [Plaintiffs] claim to have suffered little more than an increased risk of future harm … of their personal information[,]" adding, the "alleged increased risk of identity theft is insufficient to support Plaintiffs' substantive claims") (citing *Shafran v. Harley-Davidson, Inc.*, 2008 WL 763177, at *3 (S.D.N.Y. Mar. 20, 2008); *Gardiner v. Walmart, Inc.*, 2021 WL 4992539, at *3, *6 (N.D. Cal. July 28, 2021) (dismissing data breach class action because plaintiff's "vague and conclusory allegations" regarding her purported injuries are "insufficient to

(Footnote Cont'd on Following Page)

where courts have found that plaintiffs have sufficiently alleged injury, each of those cases is distinguishable from this case.[9]

Here, Plaintiffs list a whole host of differing injuries that they allegedly suffered as a result of the Security Incident, none of which could plausibly have occurred if Plaintiffs' "Social Security numbers or credit and debit card numbers" or other sensitive financial information was not affected. *See* Gilman Decl. at

---

establish the damages element required for her . . . claims."); *Sallie Holly v. Alta Newport Hosp., Inc*., 2020 WL 6161457, at *5 (C.D. Cal. Oct. 21, 2020) ("Accordingly, the Court again finds Holly's conclusory and vague allegations insufficient to establish that she suffered actual damages as a result of the data breach."); *Hammer v. Sam's E., Inc.*, 2013 WL 3756573, at *3 (D. Kan. July 16, 2013) (increased risk of identity theft is a "future-oriented, hypothetical, and conjectural" claim); *Ruiz v. Gap, Inc.*, 622 F. Supp. 2d 908, 916 (N.D. Cal. 2009), *aff'd*, 380 F. App'x 689, 693 (9th Cir. 2010).

[9] *See, e.g., In re: Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 454-55, 494-95 (D. Md. 2020) (finding damages adequately pled where plaintiffs alleged theft of highly sensitive information, including payment card information and passport numbers); *In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d 1295, 1308, 1315-17 (N.D. Ga. 2019) (finding legally cognizable injury where data breach affecting "almost half of the entire American population" involved theft of 145.5 million Social Security numbers, 17.6 million driver's license numbers, and hundreds of thousands of credit card numbers); *In re Premera Blue Cross Customer Data Sec. Breach Litig.*, 198 F. Supp. 3d 1183, 1187-89, 1206 (D. Or. 2016) (finding damages claims sufficient at pleadings stage where plaintiffs alleged theft of Social Security numbers, financial information, and protected health information); *In re Anthem, Inc. Data Breach Litig.*, 2016 WL 3029783, at *2, 12-16, 22-26 (N.D. Cal. May 27, 2016) (allowing certain damages theories to proceed where plaintiffs alleged theft of broad range of sensitive personal and health information, including patients' Social Security numbers and medical records).

Ex. A, Notice. These injuries include: (1) loss of value of their PII; (2) benefit of the bargain damages; (3) actual identity theft and fraud; (4) prophylactic (i.e. preventative) and mitigation expenses; (5) lost time; (6) increased spam emails and calls; and (7) risk of future identity theft. *See* Appendix 1 (Alleged Harm Chart). But none of these alleged harms are cognizable because, for the reasons stated below, Plaintiffs have failed to properly plead the requisite injury or damages. Accordingly, their claims must be dismissed.

*1. Plaintiffs' Claimed Diminished Value of Their Own PII Fails*

Plaintiffs claim injury in the form of "loss of value" of their PII. (Am. Compl. ¶¶ 12-13.) But "general allegations that a plaintiff's personal information has diminished in value are not enough." *Griffey v. Magellan Health Inc.*, 562 F. Supp. 3d 34, 45 (D. Ariz. 2021). "In order to survive a motion to dismiss on this theory of damages, a plaintiff 'must establish both the existence of a market for her personal information and an impairment of her ability to participate in that market.'" *Pruchnicki*, 439 F. Supp. 3d at 1234 (quoting *Svenson v. Google, Inc.*, 2016 WL 8943301, at *9 (N.D. Cal. Dec. 21, 2016)); *see also Wallace v. Health Quest Sys., Inc.*, 2021 WL 1109727, at *8 (S.D.N.Y. Mar. 23, 2021) ("[Diminished value of PII] allegations are actionable only if the plaintiff also alleges the existence of a market for that information and how the value of such information

could have decreased due to its disclosure."). Plaintiffs plead neither here.

"[T]here are no specific allegations that [P]laintiff[s] ha[ve] been unable to sell, profit from, or otherwise monetize [their] personal information." *Pruchnicki*, 439 F. Supp. 3d at 1235. Similarly, "there are no specific allegations suggesting how the value of [their] personal information has been reduced." *Id.* Likewise, Plaintiffs do "not allege that [they] tried to sell [their] information and w[ere] prevented from doing so." *Id.* Finally, Plaintiffs do not even try to establish the alleged value of their personal information let alone a reduction in the same. As such, Plaintiffs do not and cannot "allege that there was a reduction in the value of [their] personal information." *Id*.

*2. Plaintiffs' Benefit of the Bargain Claim Is Not Cognizable*

Plaintiffs allege they "would not have purchased certain products from Samsung, would have paid less for the products or services they bought from Samsung, and/or would not have provided some or all of their PII to Samsung" had they known this "would result in their PII being compromised and exfiltrated." (Am. Compl. ¶ 22.) These "benefit of the bargain" damages are routinely rejected in the data breach context where—like here—Plaintiffs fail to plead that they paid for a specific level of data security or that a specific portion of their payment went to data security. *See, e.g.*, *Dieffenbach v. Barnes & Noble, Inc.*, 887 F.3d 826, 829

(7th Cir. 2018) (finding that where the "[plaintiff] does not contend that any of the items she purchased was defective or that Barnes & Noble promised any particular level of security, for which she paid," the benefit of the bargain "is not a loss"); *Attias v. CareFirst, Inc.*, 365 F. Supp. 3d 1, 13 (D.D.C. 2019) (finding no cognizable harm based on a benefit of the bargain theory where plaintiffs alleged "that some indeterminate amount of their health insurance premiums went towards providing data security"); *Irwin v. Jimmy John's Franchise, LLC*, 175 F. Supp. 3d 1064, 1072 (C.D. Ill. 2016) ("[Plaintiff] paid for food products. She did not pay for a side order of data security and protection[.]").

Aside from general references to Samsung's various privacy notices, Plaintiffs have not alleged that Samsung represented that the cost of data security was included in the cost of products in any agreement or otherwise. *See Gardiner v. Walmart Inc.*, 2021 WL 4992539, at *5 (N.D. Cal. July 28, 2021) (finding no basis for the alleged benefit of the bargain damages where the defendant's privacy policy "never discusse[d] product pricing or charges for data security"). Such a theory is simply not viable absent "the presence of a security agreement concerning consumer data or some other representation that the cost of security is subsumed within the cost of goods. *Ables v. Brooks Bros. Grp.*, 2018 WL 8806667, at *7 (C.D. Cal. June 7, 2018).

*3. Plaintiffs' Allegations of Actual Identity Theft are Implausible, Insufficiently Pled, and Not a Cognizable Injury Absent Economic Loss*

a. The Data Elements Involved Cannot Plausibly Lead to Actual Identity Theft

Thirty-four Plaintiffs claim to have suffered "actual identity theft crimes, fraud, and other misuse" of their PII. (Am. Compl. ¶ 285; *see* Appendix 1.) Yet not a single one alleges how the "actual identity theft crimes, fraud, and other misuse" of their PII of which they complain could possibly, much less plausibly, be accomplished using the data actually impacted by the Security Incident. *Id*.

As noted above, Samsung's Notice regarding the Security Incident—which is incorporated by reference in the Complaint—specifically states that the Security Incident "***did not impact Social Security numbers or credit and debit card numbers***" and only "may have affected information such as name, contact and demographic information, date of birth, and product registration information." *See* Gilman Decl. at Ex. A, Notice (emphasis added).[10]

[10] The Court may "properly look beyond the complaint to . . . documents referenced and incorporated in the complaint and documents referenced in the complaint or essential to a plaintiff's claim which are attached to a defendant's motion," such as Samsung's Notice. *Green v. Potter*, 687 F. Supp. 2d 502, 509 n.5 (D.N.J. 2009).

Plaintiffs utterly fail to explain this logical leap from Samsung's explicit Notice that the Security Incident "did not impact Social Security numbers or credit and debit numbers" to their allegations of injury that could only result from an incident where the information impacted is of the type that can plausibly "be used to perpetrate identity theft or fraud" including "social security numbers, taxpayer identification numbers, banking information, credit card numbers, driver's license numbers, sensitive tax forms, and passport numbers." *Clemens*, 48 F.4th at 157. Indeed, Plaintiffs must specify how their alleged injuries could possibly, much less plausibly, be caused using only their "name, contact and demographic information, date of birth, and product registration information." (Am. Compl. ¶ 213.) Yet Plaintiffs proffer no plausible explanation for how harm such as fraudulent charges, compromised social media accounts, and fraudulent hospital bills could be linked to the basic—and in many cases, already public—information involved in the Security Incident. For example, Plaintiff Harold Nyanjom alleges that he experienced "unauthorized charges on his AT&T account" following the Security Incident (*id.* ¶ 94), but he does not suggest that he provided his AT&T account credentials to Samsung, much less that this information was affected by the Security Incident. Similarly, Plaintiff Erica Fletcher alleges "misuse of her PII on Instagram" (*id.* ¶ 34), but she does not claim that Samsung has access to her

Instagram account. Without such explanations, Plaintiffs' claims fail. *See, e.g.*, *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 32 (D.D.C. 2014) (finding that Plaintiffs failed to offer a plausible explanation for how allegations of fraudulent charges could be causally linked to a breach that did not impact the information necessary to carry out such harm).

Plaintiffs attempt to avoid this dispositive problem by ignoring Samsung's Notice and relying on crafty pleading and conclusory allegations to manufacture a strained link between their alleged injuries and the Security Incident. First, Plaintiffs allege that Samsung collects "an enormous volume" of highly sensitive data from its customers when they purchase Samsung products or sign up for a Samsung account, such as "social security numbers," "payment card information," "driver's license numbers," "geolocation data," "personal health information," and "username and password for participating third-party devices, apps, features, or services." (*Id.* ¶¶ 184-91.) But, notably, no Plaintiff specifically alleges that he or she gave this information to Samsung, or why and when such information would be given. Instead, Plaintiffs reliance on high level allegations that cannot be tied to any specific Plaintiff is not sufficient.

Next, Plaintiffs take a similar approach to defining "PII." Instead of outlining the specific personally identifiable information that they provided

Samsung and that they believe was impacted by the incident, Plaintiffs instead broadly define "PII" to include a laundry list of personal information including "Social Security numbers," "payment card information," and "geolocation data." (*Id.* ¶ 1.) Plaintiffs then rely on this definition to indiscriminately allege that Samsung "gathered Plaintiff[s'] . . . PII," all while (again) failing to allege the specific information that each Plaintiff supposedly provided to Samsung. (*See, e.g.*, *id.* ¶ 33.) As a result, the Court is unable to determine whether the information provided is even capable of giving rise to Plaintiffs' alleged harms.

Finally, Plaintiffs allege "upon information and belief," and in the face of contrary evidence relied on in the Complaint, that the information impacted by the Security Incident included "Social Security numbers, payment card information . . . and geolocation data." (*Id.* ¶ 26.) This is despite the Notice stating explicitly that Social Security numbers and payment card information were ***not*** involved. And with no mention of geolocation data being involved either. *See Steckman v. Hart Brewing, Inc.*, 143 F.3d 1293, 1295-96 (9th Cir. 1998) ("[W]e are not required to accept as true conclusory allegations which are contradicted by documents referred to in the complaint."); *Pickett*, 2012 WL 1601003, at *4 (observing that courts are not required to "turn a blind eye to the facts as shown in documents . . . appropriately considered in deciding a motion to dismiss if those facts directly

contradict the conclusory allegations in the complaint").

Plaintiffs cannot rely on conclusory allegations to manufacture a basis to contend that information that could, possibly, be used to perpetrate identity theft or fraud was somehow affected by the Security Incident, particularly in the face of Samsung's unequivocal disclosure to the contrary. Nor can Plaintiffs rely on broad, indiscriminate pleading to avoid alleging the specific facts necessary to plausibly allege that they provided such sensitive information to Samsung in the first place. Indeed, not a single Plaintiff alleges with any specificity that they provided Samsung with their Social Security number or credit and debit card information. Without more, Plaintiffs' claims must be dismissed. *See, e.g.*, *Jackson v. Loews Hotels, Inc.*, 2019 WL 6721637, at *4 (C.D. Cal. July 24, 2019) ("Here, Plaintiff has once again failed to demonstrate that her name, phone number, email address (but not her email password), and mailing address are sensitive enough pieces of information to give rise to a certainly impending risk of future identity theft or fraud."); *In re Horizon Healthcare Servs., Inc. Data Breach Litig.*, 2015 WL 1472483, at *7-8 (D.N.J. Mar. 31, 2015), *vacated on other grounds sub nom. In re Horizon Healthcare Servs. Inc. Data Breach Litig.*, 846 F.3d 625 (3d Cir. 2017) (finding that Plaintiff failed to "demonstrate a causal connection" because the "facts of this case demonstrate the remote possibility,

rather than the plausibility, that the [alleged harm] was connected to the [breach]."); *Ables v. Brooks Bros. Grp.*, 2018 WL 8806667, at *5 ("Assuming, without deciding, that a third party intends to commit identity theft using Ables' compromised PII, Ables still has not made allegations that give rise to the reasonable inference that the stolen PII is sufficient to actually commit identity theft."); *Stasi v. Inmediata Health Grp. Corp.*, 2020 WL 2126317, at *5 (S.D. Cal. May 5, 2020) ("Even if Plaintiffs had alleged their individual names, addresses, dates of birth, gender, and medical claims information were exposed, Plaintiffs do not allege, and cite no caselaw supporting, this information is of the type needed to open accounts or spend money in the plaintiffs' names.").

b. Identity Theft, Without More, Is Not a Cognizable Injury

Even if Plaintiffs could show that identity theft could plausibly be accomplished using the data elements actually impacted by the Security Incident (they cannot), the vast majority of these Plaintiffs fail to allege any actual or specific out-of-pocket losses as a result of this supposed harm.

For example, 18 Plaintiffs simply allude to fraudulent activity, relying on generalized allegations that they suffered "unauthorized charges" on their "accounts." (*See, e.g.*, Am. Compl. ¶ 40; *see* Appendix 1.) Plaintiffs do this without alleging the date on which any fraudulent charges were made or that they

had not been reimbursed for those charges. These are meaningful and fatal omissions. Everyone with a credit card knows that charges made without authorization are reversed by the credit card company. Thus, it is no surprise that courts have consistently found that "mere allegation[s] of an unauthorized charge, unaccompanied by an out-of-pocket loss, is not sufficient to state an actionable injury." *In re SuperValu, Inc., Customer Data Sec. Breach Litig.*, 2018 WL 1189327, at *11 (D. Minn. Mar. 7, 2018), *aff'd sub nom. In re SuperValu, Inc.*, 925 F.3d 955 (8th Cir. 2019); *Torres v. Wendy's Co.*, 195 F. Supp. 3d 1278, 1282-83 (M.D. Fla. 2016) (plaintiff who did not allege "charges went unreimbursed by his credit union" had "not alleged any monetary harm" from fraudulent charges).

Indeed, all but one of these Plaintiffs (*See* Am. Compl. ¶ 178 (Steven Baker); *see* Appendix 1) fail to allege any theft or fraud where any charge to the Plaintiff that was not ultimately reversed or resulted in the expenditure by the Plaintiff of any non-reimbursed funds. *Whalen v. Michael Stores Inc.*, 153 F. Supp. 3d 577, 580-81 (E.D.N.Y. 2015) (plaintiff lacked standing in data breach case where there where "no allegations that [she] was required to pay the [fraudulent] charges,"), *aff'd*, 689 F. App'x 89 (2d Cir. 2017). Plaintiffs' failure to allege any actual out-of-pocket loss as a result of these alleged unauthorized charges is not by mistake, as it is well understood that reversed or reimbursed

charges are insufficient to confer adequate cognizable injury. *See, e.g.*, *Torres*, 195 F. Supp. 3d at 1283 (dismissing case where plaintiff "ha[d] not alleged that the two fraudulent charges went unreimbursed by his credit union and ha[d] experienced no additional actual harm since then"); *Provost v. Aptos, Inc.*, 2018 WL 1465766, at *3 (N.D. Ga. Mar. 12, 2018) (no injury to plaintiff where she failed to allege that "she requested reimbursement from her bank or that she was denied such reimbursement"); *In re Hannaford Bros. Co. Customer Data Sec. Breach Litig.*, 613 F. Supp. 2d 108, 133-34 (D. Me. 2009) (holding that reimbursed charges cannot sustain an injury in tort or contract), *rev'd on other grounds sub nom. Anderson v. Hannaford Bros. Co.*, 659 F.3d 151 (1st Cir. 2011); *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 903 F. Supp. 2d 942, 963 (S.D. Cal. 2012) (stating that reimbursed charges were insufficient to adequately plead a cognizable injury). This failure is fatal to their claims.

Several Plaintiffs also claim to have suffered other idiosyncratic "misuse" of their PII in the form of, among others:

- Notice that a "credit card was opened in [Plaintiff's] name . . . and that [Plaintiff's] social security number was used."
- "[U]nauthorized openings of email accounts in [Plaintiff's] name"

- "[F]raudulent loan applications in [Plaintiff's] name as well as fraudulent bills"

(Am. Compl. ¶¶ 76, 100, 148.) These claims suffer the same infirmity as Plaintiffs' bare allegations regarding unauthorized charges, as Plaintiffs fail to allege any out-of-pocket loss as a result of the alleged misuse. *See, e.g.*, *Krottner v. Starbucks Corp.*, 406 F. App'x 129, 131 (9th Cir. 2010) ("[Plaintiff] alleges no loss related to the attempt to open a bank account in his name."); *Savidge v. Pharm-Save, Inc.*, 2017 WL 5986972, at *4 (W.D. Ky. Dec. 1, 2017) (finding no cognizable injury from the filing of a fraudulent tax return that the IRS did not process); *cf. Kuhns v. Scottrade, Inc.*, 868 F.3d 711, 718 (8th Cir. 2017) (holding plaintiff failed to allege actual damage where, although plaintiff alleged misuse of his data, he did not allege that he suffered "fraud or identity theft that resulted in financial loss from the use of [his] stolen PII").

*4. Expenditures on Alleged Prophylactic and Mitigation Measures Are Not Cognizable Injuries*

Twenty Plaintiffs claim to have suffered damages arising from expenditures incurred allegedly in response to the Security Incident, including "out-of-pocket expenses associated with preventing, detecting, and remediating identity theft, social engineering, and other unauthorized use of their PII," and the cost of purchasing "identity theft insurance and credit monitoring services." (Am. Compl.

¶¶ 12, 28.) Although out-of-pocket costs may be cognizable, Plaintiffs must establish that such costs were both reasonable and necessary. *Griffey*, 562 F. Supp. 3d at 45 ("Even with out-of-pocket expenses, paying for additional credit monitoring services requires 'a plaintiff to plead that the monitoring costs were both reasonable and necessary.'") (quoting *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 970 (S.D. Cal. 2014), *order corrected*, 2014 WL 12603117 (S.D. Cal. Feb. 10, 2014)). Plaintiffs, however, "offer[] no factual allegations in support of the alleged credit monitoring services, nor do[] [they] sufficiently allege that such services were reasonable and necessary." *Gardiner*, 2021 WL 2520103, at *6; *see also Holly v. Alta Newport Hosp., Inc.*, 612 F. Supp. 3d 1017, 1027 (C.D. Cal. 2020) (plaintiff's "conclusory allegations concerning any mitigation or remediation efforts fail because she has not provided any supporting factual allegations or alleged how any credit monitoring was reasonable and necessary").

Plaintiffs cannot show expenditures on credit monitoring or other prophylactic measures are reasonable, much less necessary. As shown above, Plaintiffs face no risk of "actual identity theft crimes, fraud, and other misuse" of their PII based on the alleged compromise of their "name, contact and demographic information, date of birth, and product registration information."

(Am. Compl. ¶¶ 213, 285.); *Jackson*, 2019 WL 6721637, at *4. To the extent Plaintiffs spent money on alleged prophylactic measures, such "injuries" are manufactured and non-compensable. *In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1216-17 (N.D. Cal. 2014); *see also Ables*, 2018 WL 8806667, at *7 ("In the absence of increased risk of future harm, neither time nor money expended by Ables to mitigate a hypothetical risk confers standing."); *Beck v. McDonald*, 848 F.3d 262, 276 (4th Cir. 2017) (plaintiffs' allegations "that they wish to enroll in, are enrolled in, or have purchased credit monitoring services . . . do not constitute an injury-in-fact").

*5. Lost Time Is Not a Cognizable Injury*

Every Plaintiff claims they lost "time spent in response to the Data Breach." (Am. Compl. ¶ 285.) Lost time alone, however, "is not a cognizable injury sufficient to support the element of damages." *Pruchnicki*, 439 F. Supp. 3d at 1233; *see also Bohnak v. Marsh & McLennan Cos., Inc.*, 580 F. Supp. 3d 21, 31 (S.D.N.Y. 2022) ("As to Plaintiffs' allegations that they have suffered loss of time and money responding to the increased risk of harm, these damages are not cognizable because they are not proximately caused by the harm of disclosure"); *Corona v. Sony Pictures Entm't, Inc.*, 2015 WL 3916744, at *4 (C.D. Cal. June 15, 2015) (lost time is "too speculative to constitute cognizable injury").

*6. Increased Spam Emails and Calls Are Not Cognizable Injuries*

Nearly half of the Plaintiffs claim to have suffered "a perceptible increase in scams/phishing emails, text messages and/or phone calls." (*See, e.g.*, Am. Compl. ¶¶ 34, 112.) But allegations regarding increased spam emails and calls simply do "not constitute an injury." *Jackson*, 2019 WL 6721637, at *4 (citing *Peters v. St. Joseph Servs. Corp.*, 74 F. Supp. 3d 847, 857 (S.D. Tex. 2015) (finding "no injury despite plaintiff receiving target[ed] physical, electronic and telephonic solicitations") (citation and quotations omitted); *Cherny v. Emigrant Bank*, 604 F. Supp. 2d 605, 609 (S.D.N.Y. 2009) ("The receipt of spam by itself, however, does not constitute a sufficient injury entitling [plaintiff] to compensable relief."). This is particularly so where—like here—Plaintiffs fail to allege that their email addresses or phone numbers were "not publicly available and therefore would have been difficult . . . to locate absent the assistance of the data thief." *Fernandez v. Leidos, Inc.*, 127 F. Supp. 3d 1078, 1086 (E.D. Cal. 2015) (quoting *In re Sci. Applications*, 45 F. Supp. 3d at 33) ("Plaintiff's allegation that he was injured when he received an increasing number of regular mail advertisements after the Data Breach targeting his medical conditions is not plausibly alleged as an injury fairly traceable to the Data Breach.").

*7. Alleged Imminent Risk of Future Harm Is Not a Cognizable Injury*

Plaintiffs also claim an "ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm" as a result of the Security Incident. (*E.g.*, Am. Compl. ¶ 285.) That claim, however, fails as a matter of law and fact.

"Alleged injuries that stem from the danger of future harm are insufficient to support" the prima facie damages elements of any of Plaintiffs' claims. *Pruchnicki*, 439 F. Supp. 3d at 1232. Moreover, courts routinely dismiss claims based on the alleged risk of future harm in light of the data elements at issue. *Jackson*, 2019 WL 6721637, at *4 (contact information: "Here, Plaintiff has once again failed to demonstrate that her name, phone number, email address (but not her email password), and mailing address are sensitive enough pieces of information to give rise to a certainly impending risk of future identity theft or fraud."); *In re Uber Techs., Inc., Data Sec. Breach Litig.*, 2019 WL 6522843, at *4 (C.D. Cal. Aug. 19, 2019) (contact information plus driver's license numbers: "Plaintiff fails to explain how gaining access to one's basic contact information and driver's license number creates a credible threat of fraud or identity theft."); *Antman v. Uber Techs., Inc.*, 2015 WL 6123054, at *10-11 (N.D. Cal. Oct. 19,

2015) (theft of names and driver's licenses, without more, is insufficient to establish a credible threat of immediate harm).

* * *

As demonstrated above, courts throughout the country have dismissed data breach class actions similar to this one based on the plaintiff's "fail[ure] to adequately allege damages stemming from a data breach of [defendant] by third parties." *Pruchnicki*, 845 F. App'x at 614. Here, Plaintiffs allegedly suffered a laundry list of supposed injuries as a result of the Security Incident, none of which could plausibly have occurred without Plaintiffs' "Social Security numbers or credit and debit card numbers" (*See* Gilman Decl. at Ex. A, Notice) or other sensitive financial information being affected by the incident. Given that such sensitive information was not affected by the Security Incident, Plaintiffs' alleged injuries are implausible and insufficiently pled. Their claims should be dismissed.

## VII. PLAINTIFFS' COMMON LAW CAUSES OF ACTION FAIL TO STATE A CLAIM

Plaintiffs allege the following common law claims: negligence (Count 1), negligence *per se* (Count 2), breach of confidence (Count 3), breach of express and implied contract (Counts 4 and 5), and unjust enrichment (Count 6).[11] As

[11] Plaintiffs lack standing to assert claims under the laws of the states where they do not reside. *See, e.g.*, *Ponzio v. Mercedes USA, LLC*, 447 F. Supp. 3d 194, 223 (D.N.J. 2020) (Plaintiffs bringing putative class actions "lack standing to assert

(Footnote Cont'd on Following Page)

explained above, all must be dismissed because Plaintiffs have failed to allege cognizable injury or damages. These claims should also be dismissed for the myriad reasons described below. Further, Plaintiffs' declaratory judgment claim (Count 7) should be dismissed because it is not a standalone cause of action and is wholly duplicative of Plaintiffs' other claims.

### A. Plaintiffs' Negligence Cause of Action Is Barred by the Economic Loss Doctrine and, Regardless, Fails to Allege Duty, Breach, or Damages

#### *1. Plaintiffs' Claims Are Barred by the Economic Loss Doctrine*

The economic loss doctrine bars the negligence claims of the Plaintiffs whose claims arise under the laws of Alaska, California, Colorado, Connecticut, Georgia, Illinois, Indiana, Iowa, Kansas, Louisiana, Maryland, Massachusetts, Michigan, Nevada, New Hampshire, New Jersey, New York, North Carolina, Ohio, Oregon, Pennsylvania, South Carolina and Texas. *See* Appendix 2 at Column B for states' laws on the economic loss doctrine.

The economic loss doctrine bars a plaintiff from recovering for purely economic losses under a tort theory of negligence, except where the economic losses arise from personal injury or property damage. *In re Michaels Stores Pin*

---

claims on behalf of unnamed plaintiffs in jurisdictions where [the named plaintiffs] have suffered no alleged injury."). This Section therefore only addresses the laws of the 34 states where Plaintiffs reside.

*Pad Litig.*, 830 F. Supp. 2d 518, 528 (N.D. Ill. 2011); *see also In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1171 (D. Minn. 2014) (quoting *In re Michaels*, 830 F. Supp. 2d at 528) (the economic loss doctrine "reflects the belief 'that tort law affords the proper remedy for loss arising from personal injury or damages to one's property . . . ."). If Plaintiffs had alleged any legally cognizable damages, their asserted damages would be economic in nature. Thus, the economic loss doctrine bars the negligence claims of the 36 Plaintiffs from the above-listed 23 states, and their claims should be dismissed.

In data breach cases, courts routinely dismiss negligence and negligence *per se* claims on economic loss rule grounds. *E.g.*, *Perdue v. Hy-Vee, Inc.*, 455 F. Supp. 3d 749, 761 (C.D. Ill. 2020) ("The economic loss doctrine bars a plaintiff from recovering for purely economic losses under a tort theory of negligence."); *Fox v. Iowa Health Sys.*, 399 F. Supp. 3d 780, 794 (W.D. Wis. 2019); *In re TJX Companies Retail Sec. Breach Litig.*, 564 F.3d 489, 499 (1st Cir. 2009), *as amended on reh'g in part* (May 5, 2009) (holding that Massachusetts state law was "clear" and that the economic loss doctrine barred plaintiffs' negligence claim).

Plaintiffs fail to allege any cognizable injury (*supra* Section VII.B), let alone any "personal injury or damages to one's property." *In re Target*, 66 F. Supp. 3d at 1171 (quoting *In re Michaels*, 830 F. Supp. 2d at 528). Because Plaintiffs only

allege economic damages, their negligence and negligence *per se* claims are barred under the economic loss doctrine in the 23 states listed above. The Court should therefore dismiss the negligence and negligence *per se* claims of the 36 Plaintiffs as barred under the economic loss doctrine. *See* Appendix 2 at Column B.

*2. Plaintiffs Fail to Allege that Samsung Owed Them a Duty*

It is axiomatic that a legal duty is a required element of any negligence claim. *See, e.g.*, *Irwin* 175 F. Supp. 3d at 1071 ("An essential element of a negligence claim is the existence of a duty owed to the plaintiff."). Plaintiffs have failed to plead this essential element.

a. Samsung does not have a duty to safeguard information from a third party

Plaintiffs allege that Samsung owed them a duty to "protect consumer data" (Am. Compl. ¶ 277), but certain states do not recognize a common law duty to protect personal information and routinely dismiss negligence claims in data breach cases on that ground alone. Thus, Plaintiffs' negligence claims cannot survive for the eight Plaintiffs in Arizona, Illinois, Oklahoma, and Washington, because those states do not recognize a duty to safeguard information from a third party. *See* Appendix 2 at Column C (listing cases).

Similarly, North Carolina and Texas have never recognized or found a common-law duty to safeguard information. *See* Appendix 2 at Column C. This

Court is not permitted to create state law that does not exist. Rather, the correct outcome is to "choose the narrower and more reasonable path" of holding that no general common-law duty exists "at least until the [state courts] tell[] us differently." *Piscotta v. Old Nat'l Bancorp*, 499 F.3d 629, 636 (7th Cir. 2007) (quoting *Todd v. Societe Bic, S.A.*, 21 F.3d 1402, 1412 (7th Cir. 1994)); *see also Gen. Fid. Ins. Co. v. Foster*, 808 F. Supp. 2d 1315, 1321 (S.D. Fla. 2011) ("[A] Federal Court sitting in diversity should not act to create or expand states public policy . . . ."). As such, this Court should also dismiss the negligence claims of the two Plaintiffs in North Carolina and Texas.

b. Samsung does not have a duty to protect Plaintiffs against unlawful conduct of criminal actors

Plaintiffs allege "[t]he Data Breach was the product of an intentional . . . criminal act" and "was the result of a sophisticated and malicious attack by professional cybercriminal hackers." (Am. Compl. ¶ 25.) Samsung, however, has no duty to protect Plaintiffs against the unlawful conduct of a third-party criminal since criminal acts are unforeseeable acts. *See Georgia CVS Pharm., LLC v. Carmichael*, 2023 WL 4247591, at *16 (Ga. June 29, 2023) (quoting *Days Inns of America v. Matt*, 454 S.E.2d 507 (Ga. 1995)) ("[W]ithout foreseeability that a criminal act will occur, no duty on the part of the proprietor to exercise ordinary care to prevent that act arises."); *Champion ex rel. Ezzo v. Dunfee*, 939 A.2d 825,

831 (N.J. Super. Ct. App. Div. 2008) ("[A]bsent a special relationship, there is no duty to control a third person's conduct."); *Brown v. Brown*, 739 N.W.2d 313, 316-19 (Mich. 2007) (holding that third-party criminal activity is "irrational and unpredictable" and that the imposition of such "a duty on defendant would not effectively further a policy of preventing future harm, and would impose an undue burden on defendant[s]."); Restatement (Second) of Torts § 314 (1965) (stating that even when one determines that his action "is necessary for another's aid or protection" that does not impose upon him a duty to take action).

Instead, as *In re Blackbaud, Inc., Customer Data Breach Litigation* recognized, there are only a few very limited exceptions to this rule. 567 F. Supp. 3d 667, 681-82 (D.S.C. 2021). In pertinent part, the plaintiff must allege: (1) a special relationship with the defendant, (2) a statutorily imposed duty on the defendant, or (3) the defendant negligently or intentionally creates the risk that results in the harm. *See id.* at 681. None of these exceptions are relevant here.

First, Plaintiffs try to allege the existence of a "special relationship" between Plaintiffs and Samsung because Plaintiffs "entrusted Samsung with their PII as part of the purchase and subsequent use of products." (Am. Compl. ¶ 274.) Plaintiffs' conclusory allegations of a "special relationship" fail as a matter of law. As courts—including the *Blackbaud* court—recognize, special relationships are

primarily confined to a few well-defined categories of relationships formed between: (1) common carriers and their passengers; (2) innkeepers and their guests; (3) possessors of land and members of the public who are their invitees; and (4) those who are required by law to take physical custody of another or who voluntarily do so. Restatement (Second) of Torts § 314A (1965); *In re Blackbaud*, 567 F. Supp. 3d at 681-82; *Champion*, 939 A.2d at 122 (stating that under New Jersey law a special relationship only exists in certain narrow instances of a "parent-child; master-servant; landlord-tenant; and guardian-ward"). It is evident from the Complaint that none of these apply here. *See Com. Bancorp, Inc. v. BK Int'l Ins. Brokers, Ltd.*, 490 F. Supp. 2d 556, 564 (D.N.J. 2007) (finding no special duty of care between "two parties to a contract"); *Gardiner*, 2021 WL 2520103, at *9 (finding that a consumer did not have a special relationship with Walmart because "Plaintiff d[id] not allege that the transaction at issue was intended to benefit Plaintiff in a specific way that set[] him apart from all potential Walmart customers"); *In re Sony*, 996 F. Supp. 2d at 969 ("Plaintiffs have failed to allege a 'special relationship' with Sony beyond those envisioned in everyday consumer transactions . . . .").

Second, the "assumption of duty doctrine" cannot apply here because Plaintiffs have not alleged any physical harm. Restatement (Second) of Torts

§ 324A (1965) ("One who undertakes, gratuitously or for consideration, to render services to another which he should recognize as necessary for the protection of a third person or his things, is subject to liability to the third person for ***physical harm*** resulting from his failure to exercise reasonable care to protect his undertaking . . . ." (emphasis added)).

Third, Plaintiffs allege that Samsung owed them a duty under Section 5 of the Federal Trade Commission Act (15 U.S.C. § 45) ("FTC Act"), and that Samsung had a duty to "provide timely, adequate, and appropriate notification of the Data Breach." (Am. Compl. ¶¶ 275, 280.) Neither establishes a statutory duty for Samsung to act. As to the FTC Act, this argument fails because the FTC Act does not create a private right of action. *See In re SuperValu, Inc.*, 925 F.3d at 963-64. For the reasons explained *infra* Section VII.B.2, Plaintiffs cannot establish duty under the FTC Act or "similar state statutes" without a private right of action. Similarly, Plaintiffs' argument with respect to the data breach statutes fail because some do not have a private right of action and, for those that do, Plaintiffs have failed to allege a violation of any state data breach notification statute. *See infra* Section IX.A-C. Regardless, Samsung notified Plaintiffs of the Security Incident, even though it was not legally obligated to notify outside North Dakota and Washington. *See supra* Section II.

Fourth, Plaintiffs do not sufficiently allege that Samsung negligently or intentionally created the risk of the incident. Plaintiffs fail to allege facts that Samsung knew of the risk of this incident. All Plaintiffs muster on this point is that "Samsung knew or should have known that its computing systems and data storage were vulnerable to unauthorized access and targeting by hackers for the purpose of stealing and misusing confidential PII." (Am. Compl. ¶ 278.) This is not sufficient. *See Attias*, 365 F. Supp. 3d at 21 (dismissing negligence claims because "plaintiffs have made no allegations that it was foreseeable that [Defendant] specifically would suffer a data breach based on, for instance, known vulnerabilities in its data-storage systems."). Plaintiffs point to no actual notice provided to Samsung that its computer systems were inadequate. Nor do they allege specific facts about why Samsung's computing systems and data storage were vulnerable to this particular incident. Instead, Plaintiffs rely merely on *ipse dixit*.

Plaintiffs' attempt to plead negligence by pointing to other security incidents is likewise unavailing because Plaintiffs do not even attempt to demonstrate how the alleged prior security incidents have any relevance to the Security Incident at issue here. (Am. Compl. ¶ 3); *cf. In re: The Home Depot, Inc., Customer Data Sec. Breach Litig.*, 2016 WL 2897520, at *3 (N.D. Ga. May 18, 2016) (holding

that Defendant had a legal duty because "Plaintiffs have pleaded that the Defendant knew about a substantial data security risk dating back to 2008 but failed to implement reasonable security measures to combat it."); *In re Arby's Rest. Grp. Inc. Litig.*, 2018 WL 2128441, at *5 (N.D. Ga. Mar. 5, 2018) ("Plaintiffs allege that Arby's knew about potential issues with its point of sale systems and failed to implement reasonable security measures.").

*3. Plaintiffs' Negligence Claims Must Be Dismissed Because Plaintiffs Fail to Allege a Breach*

Even assuming that Samsung had a duty to Plaintiffs, which it did not, Plaintiffs' negligence claims should be dismissed because Plaintiffs fail to allege that a breach proximately caused their alleged harm. *See Brunson v. Affinity Fed. Credit Union*, 972 A.2d 1112, 1122-23 (N.J. 2009); *In re Equifax, Inc.*, 362 F. Supp. 3d at 1317-18. Despite the Complaint's length, Plaintiffs do not plausibly explain any specific failures that allegedly allowed the Security Incident to occur. Plaintiffs also fail to plead how Samsung's security measures were deficient or in what way Samsung was not in compliance with general cybersecurity standards. Instead, Plaintiffs ask this Court to assume that because an incident happened, Samsung must have failed to "implement data management and security measures sufficient to protect that data and comply with industry standards." (Am. Compl. ¶ 11.)

Plaintiffs' lack of specificity is dispositive. "[T]he law does not impose strict liability for harms arising out of the storage of personal information." *In re Waste Mgmt. Data Breach Litig.*, 2022 WL 561734, at *5 (S.D.N.Y. Feb. 24, 2022); *see also Lovell v. P.F. Chang's China Bistro, Inc.*, 2015 WL 4940371, at *5 (W.D. Wash. Mar. 27, 2015).

The Complaint contains many allegations of general security measures that Plaintiffs consider inappropriate and many conclusory assertions that Samsung failed to take reasonable measures to protect the data. (*See, e.g.*, Am. Compl. ¶¶ 10, 198.) However, the Complaint fails to plead any ***facts*** regarding specific measures that Samsung should have taken, but did not, or how those measures would have prevented a successful criminal attack. Plaintiffs' conclusory allegations of breach are nothing more than "labels and conclusions," *Twombly*, 550 U.S. at 555, and courts have not hesitated to dismiss cases with similarly threadbare allegations. *See, e.g.*, *Kuhns*, 868 F.3d at 717-18 (affirming dismissal of complaint when it "left [the court] to guess" how the "security measures" were deficient); *In re Waste Mgmt.*, 2022 WL 561734, at *5.

### B. Plaintiffs' Negligence *Per Se* Cause of Action Fails[12]

#### *1. Negligence per se is not an independent cause of action in certain states*

In Alabama, California, Michigan, and Pennsylvania,[13] negligence *per se* is not an independent cause of action. *See* Appendix 2 at Column D (listing cases). Thus, the negligence *per se* claims (Count 2) for the seven Plaintiffs in these four states fail. *Id.*

#### *2. Plaintiffs' claims fail because the FTC Act, and "state data security statutes," cannot serve as a basis for negligence per se*

Plaintiffs assert claims of negligence *per se*—a theory that permits plaintiffs to establish duty and breach by proving that a defendant violated a statutory standard of conduct—based on violations of the FTC Act and "state data security statutes." (Am. Compl. ¶¶ 286-97.) But, in at least 18 states,[14] alleged violations of the FTC Act cannot form the basis of a negligence *per se* claim because the FTC

---

[12] As explained in Section VII.A.1, the economic loss doctrine bars the negligence *per se* claims for the 36 Plaintiffs in the 23 states discussed therein.

[13] Negligence *per se* is also not an independent cause of action in Arkansas, Louisiana, Maryland, Massachusetts and Oregon, but Plaintiffs are not bringing a negligence *per se* claim under the laws of those states. (*See* Am. Compl. at p. 115, n.56.)

[14] *See* Appendix 2 at Column E showing that Arizona, California, Colorado, Florida, Illinois, Indiana, Kansas, Minnesota, Nevada, New Jersey, New Mexico, New York, North Carolina, Ohio, Oklahoma, South Carolina, Tennessee, and Wisconsin require a private right of action for a negligence *per se* claim.

Act does not have a private right of action. *See, e.g.*, *In re Mednax Servs., Inc.*, *Customer Data Sec. Breach Litig.*, 603 F. Supp. 3d 1183, 1225 (S.D. Fla. 2022) (citation omitted) ("There is no private cause of action implied under the Federal Trade Commission Act. . . . Thus, violations of Section 5 cannot form the basis for a negligence *per se* claim."); *In re GE/CBPS Data Breach Litig.*, 2021 WL 3406374, at *10 (S.D.N.Y. Aug. 4, 2021) ("negligence *per se* claim is not viable . . . because [the FTC Act] does not provide a private right of action; instead the FTC confers exclusive enforcement authority on the Federal Trade Commission"); *Green v. 712 Broadway, LLC*, 2018 WL 2754075, at *7 (D.N.J. June 8, 2018) (negligence *per se* claim cannot survive if the underlying statute does not create a private right of action).

Courts across the country have held that a negligence *per se* claim cannot rest on a federal statute that does not provide a private right of action, such as the FTC Act. *See* Appendix 2 at Column E (listing cases). Additionally, the FTC Act cannot serve as a basis for Plaintiffs' negligence *per se* claims because it does not impose strict liability in tort. And because Plaintiffs "do[] not allege violation of a statute that imposes strict liability," the Court should dismiss the claim. *Toretto v. Donnelley Fin. Sols., Inc.*, 583 F. Supp. 3d 570, 598 (S.D.N.Y. 2022) (dismissing plaintiffs' negligence *per se* claim on the ground that the FTC Act does not impose

strict liability).[15]

Plaintiffs also rely on "similar state statutes" as a basis for their negligence *per se* claim. (Am. Compl. ¶ 291). However, Plaintiffs fail to allege the specific "state statutes" that serve as the basis for their negligence *per se* claim. *Id.* Courts routinely dismiss negligence *per se* claims where plaintiffs fail to "cite a specific statute" because it does not "adequately put Defendant on notice about the legal nature of the negligence per se claim." *Almanzar v. Eaglestar*, 2021 WL 7184209, at *6 (W.D. Tex. Dec. 21, 2021) (collecting cases); *Santa Clarita Valley Water Agency v. Whittaker Corp.*, 2021 WL 6104175, at *2 (C.D. Cal. Dec. 3, 2021) (quoting *Bock v. Cty. of Sutter*, 2012 WL 3778953, at *16 (E.D. Cal. Aug. 31, 2012) ("Relatedly, courts consistently reject negligence per se claims that fail to specify the 'specific statute, ordinance, or regulation in support of their claim.'"). To the extent that Plaintiffs intend to rely on the state statutes included in Counts 8 through 61, the Court should dismiss the negligence *per se* claims for the reasons

[15] For the states that either allow negligence *per se* claims where the underlying statute does not have a private right of action, or where state courts have not yet addressed this issue, Plaintiffs' negligence *per se* claim still fails because: (1) the claim is barred by the economic loss doctrine (*see* Section VII.A.1 and Appendix 2, Column B); (2) the state does not recognize negligence *per se* claims (*see* Section VII.B.1 and Appendix 2, Column D); or (3) the state only recognizes negligence *per se* claims in limited circumstances not applicable here (*see* Section VII.B.3 and Appendix 2, Column F).

explained *infra* Sections VIII through X.

*3. For the few states where it is unsettled on whether the FTC Act can serve as a basis, Plaintiffs' negligence per se claims fail because they are only recognized in limited circumstances not applicable here*

Plaintiffs' negligence *per se* claims in Connecticut, Georgia, Texas and Washington fail because these states only recognize the claim in limited circumstances that are not applicable here.

In Connecticut and Georgia, a statute must have an ascertainable standard of conduct to support a negligence *per se* claim. *Wells Fargo Bank, N.A. v. Jenkins*, 744 S.E.2d 686, 688 (Ga. 2013); *Hummock Island Shellfish, LLC v. Birchwood Country Club, Inc.*, 2018 WL 1137534, at *3 (Conn. Super. Ct. Jan. 26, 2018). In Connecticut, courts have declined to find negligence *per se* where the "statutes upon which the plaintiff relies do not provide specific standards pursuant to which a party engaged in a particular activity must conform its conduct," but rather only "include broad policy statements." *Hummock Island Shellfish*, 2018 WL 1137534, at *3. The FTC Act—which broadly prohibits "unfair trade practices"—does not provide an ascertainable standard of conduct, and so it cannot be the basis for creating a duty to protect personal information such as the Plaintiffs would have the Court create here.

For Georgia, in *Wells Fargo Bank*, the plaintiff brought tort claims based on the Gramm-Leach-Bliley Act, which requires financial institutions "to protect the security and confidentiality of [] customers' nonpublic personal information." 744 S.E.2d at 687 (quoting 15 U.S.C. § 6801(a)). The Georgia Supreme Court held this statute could not support a tort duty to protect customers' information because "[i]t does not provide for certain duties or the performance of or refraining from any specific acts on the part of financial institutions, nor does it articulate or imply a standard of conduct or care, ordinary or otherwise." *Id.* at 688; *see also Dep't of Labor v. McConnell*, 828 S.E.2d 352, 358 (Ga. 2019) (declining to impose a tort duty to safeguard personal information under a state statute that "d[id] not explicitly establish any duty, nor . . . prohibit or require any conduct at all."). Thus, the FTC Act cannot be the basis for a negligence *per se* claim in Georgia.

In Texas, negligence *per se* is not available for violations of statutes that are "not penal in nature." *Ridgecrest Ret. & Healthcare v. Urban*, 135 S.W.3d 757, 762-63 (Tex. Ct. App. 2004). The FTC Act is not a penal statute, and, thus, no claim for negligence *per se* is permitted for its violation in Texas. *See Boales v. Brighton*, 29 S.W.3d 159, 166 (Tex. Ct. App. 2000).

In Washington, negligence *per se* is available only for "breach of a rule relating to electrical fire safety, the use of smoke alarms, or driving while under the

influence," *Buchanan v. Simplot Feeders, LLC*, 2019 WL 7763826, at *2 (E.D. Wash. Oct. 29, 2019), which is indisputably irrelevant to the FTC Act.

Accordingly, for the reasons stated above, this Court should dismiss the negligence *per se* claims of the five Plaintiffs in Connecticut, Georgia, Texas and Washington because these states only recognize the claim in limited circumstances that are not applicable here. *See* Appendix 2 at Column F (listing cases).

### C. Plaintiffs' Breach of Confidence Cause of Action Fails

#### *1. In certain states, breach of confidence is either not a recognized cause of action, or has only been recognized in narrow circumstances not applicable here*

Breach of confidence is not a recognized cause of action in Colorado, Indiana, Kansas, New Jersey, North Carolina, and Texas.[16] *See* Appendix 3 at Column C (listing cases).

In other states, including Alabama, Alaska, Arkansas, Connecticut, Florida, Iowa, Michigan, Minnesota, New York, Ohio, Oklahoma, and Rhode Island, breach of confidence claims have been recognized only in narrow circumstances that are not applicable here, such as disclosure of medical information or trade secrets. *See id.* at Column D (listing cases). Finally, several states, including

[16] Plaintiffs are not bringing their breach of confidence claim under the laws of Illinois, Maryland, South Carolina, Washington or Wisconsin. (Am. Compl. at p. 117 n.57.)

Alaska, Arizona, California, Georgia, Iowa, Louisiana, Massachusetts, Minnesota, Nevada, New Hampshire, New Mexico, New York, Oregon, Pennsylvania, and Tennessee require a duty of confidentiality or confidential relationship between the parties (not simply an arms' length business transaction). *See id.* at Column E (listing cases). Plaintiffs fail to allege that any of these narrow circumstances apply here.

For these reasons, the breach of confidence claims must be dismissed.

*2. Plaintiffs' breach of confidence claims also fail because there was no disclosure*

In order to establish a breach of confidence claim, a plaintiff must sufficiently allege a disclosure. *See Kamal v. J. Crew Grp., Inc.*, 918 F.3d 102, 114 (3d Cir. 2019). A disclosure is "[t]he act or process of making known something that was previously unknown." *In re Brinker Data Incident Litig.*, 2020 WL 691848, at *22 (M.D. Fla. Jan. 27, 2020) (alteration in original) (quotation marks omitted). A disclosure does not happen where a defendant's "[alleged] inadequate security facilitated the theft" of information by a third party." *Id.* Instead, a plaintiff must allege that the defendant affirmatively shared plaintiffs' information or performed an act that made the plaintiffs' information known. *See In re Ambry Genetics Data Breach Litig.*, 567 F. Supp. 3d 1130, 1147 (C.D. Cal. 2021) (holding plaintiffs had not alleged a claim for breach of confidence where

the Complaint "[did] not allege that Defendants affirmatively shared any information or performed any act that gave hackers information").

It is undisputed that Samsung did not disclose Plaintiffs' information into the public domain. (Am. Compl. ¶ 25 ("[the attack] was the result of a sophisticated and malicious attack by professional cybercriminal hackers ***and was not the result of an accidental disclosure by a Samsung employee***.") (emphasis added)). Courts have summarily dismissed breach of confidence claims in data breach cases where information was stolen by third-parties. *See In re Brinker*, 2020 WL 691848, at *22 ("'disclosure' is '[t]he act or process of making known something that was previously unknown.' . . . But Brinker did not do any act that made Plaintiffs' information known—the information was stolen by third-parties.") (alteration in original) (quoting *Disclosure*, *Black's Law Dictionary* (11th ed. 2019)); *see also In re Ambry*, 567 F. Supp. 3d at 1147 (holding plaintiffs had not alleged a claim for breach of confidence where they "[did] not allege that Defendants affirmatively shared any information or performed any act that gave hackers information."); *Foster v. Health Recovery Servs., Inc.*, 493 F. Supp. 3d 622, 636 (S.D. Ohio 2020) (holding that plaintiff failed to state a claim for breach of confidence because "what is alleged is that a third party has exploited Defendant's security weakness to access the information without Defendant's

authorization"). This Court should do the same and dismiss Plaintiffs' breach of confidence claims.

### D. Plaintiffs' Breach of Contract and Breach of Implied Contract Causes of Action Fail

To state a claim for breach of contract, a plaintiff must allege: (1) the existence of a valid contract between the parties, (2) plaintiff's performance of their own obligations under that contract, (3) a defective or deficient performance under the contract by the defendant, and (4) damages resulting from the breach.[17] *E.g.*, *Powell v. Seton Hall Univ.*, 2022 WL 1224959, at *8 (D.N.J. Apr. 26, 2022). "The only difference between an implied-in-fact contract and an express contract is that the parties' agreement has been manifested by conduct instead of words." *E.g.*, *Duffy v. Charles Schwab & Co.*, 123 F. Supp. 2d 802, 816-17 (D.N.J. 2000).

There is no valid contract that Samsung could have "breached" because Samsung did not assume a contractual obligation to protect Plaintiffs' PII. And even if Samsung had assumed a contractual duty concerning cybersecurity, Plaintiffs do not adequately allege that Samsung breached that duty. Plaintiffs' contract claims (Counts 4 and 5) must be dismissed.

[17] *See* Appendix 4 for states' laws on the damages element of breach of contract and breach of implied contract claims.

*1. Samsung's privacy policy is not an enforceable contract*

Plaintiffs allege they formed a contract with Samsung by obtaining products or services from Samsung subject to its Privacy Policy (*e.g.*, Am. Compl. ¶¶ 308, 319). But courts across the country recognize that corporate privacy policies are not enforceable contracts where, like Samsung's Privacy Policy, they contain only broad statements about corporate policy provided for informational purposes to help individuals understand how Samsung may use their personal information.[18] Samsung's customers are not required to agree to the Privacy Policy and it imposes no obligations on them. *See In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 611 (9th Cir. 2020) (no contract where, like here, policy "provides information—not commitments—regarding [company's] use of information").

[18] *See, e.g.*, *Jurin v. Google Inc.*, 768 F. Supp. 2d 1064, 1073 (E.D. Cal. 2011) (dismissing breach of contract claims arising out of the alleged breach by Google of its AdWords policy terms and conditions on the ground that a "broadly stated promise to abide by its own policy does not hold Defendant to a contract"); *Dyer v. Nw. Airlines Corps.*, 334 F. Supp. 2d 1196, 1200 (D.N.D. 2004) (holding that plaintiffs could not maintain suit against Northwest Airlines for breach of its privacy statement because it was not a contract); s*ee also Meyer v. Christie*, 2007 WL 3120695, at *4-5 (D. Kan. Oct. 24, 2007) (noting that unilateral corporate policies generally do not support breach of contract claims).

(Footnote Cont'd on Following Page)

In addition, "[c]ontracts must be supported by consideration." *Rusnack v. Cardinal Bank, N.A.*, 695 F. App'x 704, 712 (4th Cir. 2017). No contract exists where a "promisor is free to perform or to withdraw from the agreement at will." *See First Wis. Nat'l Bank of Milwaukee v. Oby*, 188 N.W.2d 454, 457 (Wis. 1971). Samsung's Privacy Policy states that Samsung "may update this Privacy Policy from time to time and without prior notice to you to reflect changes in our personal information practices with respect to the Services."[19]

*2. Plaintiffs fail to allege breach of the privacy policy*

Even if Plaintiffs can establish the existence of a contract, Plaintiffs have not plausibly alleged that Samsung breached any purported contractual obligation to protect their PII. Plaintiffs' claims are based on alleged "promises" that Samsung made in its Privacy Policy. (Am. Compl. ¶¶ 308, 319.) According to Plaintiffs, Samsung agreed "that it would only share data under certain enumerated

[19] *Samsung Privacy Policy for the U.S.*, Samsung (Dec. 30, 2022), https://www.samsung.com/us/account/privacy-policy/; *see also Privacy Notice: Samsung Privacy Policy for the U.S.*, Samsung (Dec. 30, 2022), https://account.samsung.com/membership/terms/privacypolicy. To decide a motion to dismiss, courts are permitted to consider a document not attached to the complaint if plaintiff's claims are based on the document. *See Pension Ben. Guar. Corp. v. White Consol. Indus., Inc.*, 998 F.2d 1192, 1196 (3d Cir. 1993). The URL for the Privacy Policy is specifically referred to in paragraph 183 of the Complaint, footnote 4 in paragraph 185 and footnote 10 in paragraph 192 of the Complaint. The Complaint refers to the Privacy Policy numerous times as well. Thus, it is proper for this Court to consider when determining Samsung's motion to dismiss.

circumstances," which did not include unauthorized access by criminal hackers. (Am. Compl. ¶ 312.) But Samsung did not "share" Plaintiffs' PII (*id.*); it was stolen. Moreover, Samsung's Privacy Policy only states that Samsung "maintain[s] safeguards designed to protect personal information." Samsung Privacy Policy for the U.S., *supra* note 19. Plaintiffs attempt to turn this into a blanket guarantee that their PII would be protected in all circumstances from third-party criminal actors. Such a reading of the Privacy Policy is wholly implausible. And, Plaintiffs do not allege that Samsung failed to abide by its promise to maintain safeguards designed to protect personal information. Thus, even if the Privacy Policy was a contract, there is no allegation that Samsung breached it.

*3. Plaintiffs' implied contract claims also fail*

Plaintiffs fail to plausibly allege the existence of any valid implied contract.[20] Under each of the potentially applicable states' laws, an implied contract requires proof of the same elements as an express contract, including

[20] Plaintiffs' implied contract claim should not stand if the Court finds that an express contract exists. *See, e.g.*, *Baer v. Chase*, 392 F.3d 609, 616-17 (3d Cir. 2004) ("There cannot be an implied-in-fact contract if there is an express contract that covers the same subject matter. In other words, express contract and implied-in-fact contract theories are mutually exclusive.").

(Footnote Cont'd on Following Page)

mutual assent, a meeting of the minds and breach.[21] Plaintiffs fail to allege any facts from which the Court could infer that Samsung and Plaintiffs impliedly agreed that Samsung would assume a duty to maintain their PII. Instead, Plaintiffs try to infer Samsung's acceptance of vague and unspecified contractual obligations about data security from the allegation that Samsung's Privacy Policy "included the promise that Samsung 'maintain[s] safeguards designed to protect personal information'" and that Samsung "made other statements to Plaintiffs and Class Members promising to ensure the security of their PII." (Am. Compl. ¶¶ 310-11.) But courts have consistently rejected this argument.[22]

---

[21] *See Dixon v. Bhuiyan*, 10 P.3d 888, 891 (Okla. 2000); *Saluteen-Maschersky v. Countrywide Funding Corp.*, 22 P.3d 804, 807 (Wash. Ct. App. 2001); *Pac. Bay Recovery, Inc. v. Cal. Physicians' Servs., Inc.*, 218 Cal. Rptr. 3d 562, 574-75 (Ct. App. 2017); *Snyder v. Freeman*, 266 S.E.2d 593, 602 (N.C. 1980); *Slick v. Reinecker*, 839 A.2d 784, 787 (Md. Ct. Spec. App. 2003); *Pyeatte v. Pyeatte*, 661 P.2d 196, 203 (Ariz. Ct. App. 1982); *see also Hercules Inc. v. U.S.*, 516 U.S. 417, 423-24 (1996).

[22] *See, e.g.*, *Krottner*, 406 F. App'x at 131 (dismissing implied-contract claim in a data-breach case under Washington law because plaintiffs failed to plausibly allege elements of a contract); *Brush v. Miami Beach Healthcare Grp.*, 238 F. Supp. 3d 1359, 1369 (S.D. Fla. 2017) (dismissing implied-contract claim because "[n]othing in the . . . Complaint gives rise to a factual inference that the Defendants tacitly agreed to secure her personal data in exchange for remuneration"); *Frezza v. Google Inc.*, 2012 WL 5877587, at *4 (N.D. Cal. Nov. 20, 2012) (dismissing implied-contract claim because plaintiffs did not "sufficiently plead that Google agreed to and then breached a specific obligation"); *Longenecker-Wells v. Benecard Servs.*, 658 F. App'x 659, 662-63 (3d Cir. 2016) (dismissing implied-contract claim in data-breach case when plaintiffs "failed to plead any facts

(Footnote Cont'd on Following Page)

As discussed *supra* Section VII.D.1, a promise to maintain reasonable safeguards to protect a customer's PII is not a promise that Samsung's systems are impenetrable to professional criminal hackers. If an implied obligation existed, it was at most to ***mitigate*** the risk of unauthorized access, not prevent it. Plaintiffs fail to allege with specificity what reasonable security procedures and practices Samsung failed to use that amounted to breach of an implied contractual obligation. "No facts are alleged to support an inference that [Samsung] even contemplated, much less agreed to meet the [security] standards" that Plaintiffs claim they were owed. *See Frezza*, 2012 WL 5877587, at *4.

Plaintiffs' allegation that some "implied contract" exists is nothing more than a bare legal conclusion entitled to no weight and should be dismissed.

### E. Plaintiffs' Unjust Enrichment Cause of Action Fails

Plaintiffs fail to state claims for unjust enrichment under the laws of each of the 34 states where they reside.

---

supporting their contention that an implied contract arose between the parties"); *Stephens v. Availity, LLC*, 2019 WL 13041330, at *6 (M.D. Fla. Oct. 1, 2019) (dismissing implied-contract claim when plaintiff failed to allege any direct relationship with the defendant (a healthcare services provider), much less a meeting of the minds as to information-security standards).

*1. Unjust enrichment is not a recognized or standalone cause of action in California, Illinois and Texas*

California, Illinois, and Texas do not recognize unjust enrichment. *See* Appendix 5 at Column B (listing cases). For this reason alone, the Court should dismiss the unjust enrichment claims of the nine Plaintiffs from these states.

*2. Plaintiffs' unjust enrichment claims fail because they fail to allege they do not have an adequate remedy at law*

In at least 25 of the states included in Plaintiffs' Complaint, courts have routinely dismissed unjust enrichment claims when plaintiffs fail to demonstrate that there is no adequate remedy at law. *See* Appendix 5 at Column C (listing cases). Here, Plaintiffs assert claims for money damages under state statutes from 34 states, as well as common law claims seeking actual and punitive damages. Plaintiffs cannot plausibly allege they do not have an adequate remedy at law. Thus, an action for unjust enrichment that sounds in equity cannot be sustained for the 39 Plaintiffs in the 25 states listed in Appendix 5 at Column C.

*3. Plaintiffs' unjust enrichment claims fail because they do not allege a "direct relationship" with Samsung*

Courts recognize that there must be some "direct relationship" between the parties, or a benefit provided by a plaintiff directly to a defendant, for an unjust enrichment claim to be viable. *See, e.g., Cooper v. Samsung Elecs. Am., Inc.*, 2008 WL 4513924, at *10 (D.N.J. Sept. 30, 2008) (dismissing unjust enrichment claim

because "there was no relationship conferring any direct benefit on [defendant] through [plaintiff's] purchase, as the purchase was through a retailer"), *aff'd*, 374 F. App'x 250 (3d Cir. 2010); *In re Keurig Green Mountain Single-Serve Coffee Antitrust Litig.*, 383 F. Supp. 3d 187, 272 (S.D.N.Y. 2019) (finding indirect purchasers' relationship to manufacturer "too attenuated to support a claim of unjust enrichment"); *Johnson v. Microsoft Corp.*, 834 N.E.2d 791, 799 (Ohio 2005) ("The rule of law is that an indirect purchaser cannot assert a common-law claim for restitution and unjust enrichment against a defendant without establishing that a benefit had been conferred upon that defendant by the purchaser."); *Kopel v. Kopel*, 229 So. 3d 812, 818 (Fla. 2017) ("[T]o prevail on an unjust enrichment claim, the plaintiff must directly confer a benefit to the defendant."). Here, while Plaintiffs allege they purchased Samsung products, they do not allege that they purchased those products directly from Samsung. Accordingly, the parties' relationship is too attenuated to state a claim for unjust enrichment.

*4. Plaintiffs have not plausibly alleged that they conferred a benefit on Samsung and did not receive what they paid for*

While the elements of unjust enrichment vary by state, "almost all states at minimum require plaintiffs to allege that they conferred a benefit or enrichment upon defendant and that it would be inequitable or unjust for defendant to accept

and retain the benefit." *In re Flonase Antitrust Litig.*, 692 F. Supp. 2d 524, 541 (E.D. Pa. 2010).[23] Plaintiffs' allegations fall flat on both elements.

First, Plaintiffs' unjust enrichment claim fails because they have not alleged that they conferred any benefit on Samsung. In their Complaint, Plaintiffs allege that they provided their personal information to Samsung. (Am. Compl. ¶¶ 328-29.) This argument fails because "[c]ourts have routinely rejected the proposition that an individual's [PII] has an independent monetary value." *Welborn v. IRS*, 218 F. Supp. 3d 64, 78 (D.D.C. 2016); *see also In re Arthur J. Gallagher Data Breach Litig.*, 631 F. Supp. 3d 573, 592 (N.D. Ill. 2022) ("Plaintiffs insist that Defendants retained the 'monetary benefit' of Plaintiffs' 'valuable PII and PHI.' . . . Courts have, however, routinely rejected the 'proposition that an individual's personal identifying information has an independent monetary value.'") (citation omitted). "If anything, the . . . complaint suggests that third-party hackers, not Defendant[], are the ones who benefitted from the Data Breach." *In re Arthur J. Gallagher*, 631 F. Supp. 3d at 592.

Second, Plaintiffs' claim fails because they have not alleged that they did not receive what they paid for, and that it would be unjust for Samsung to retain any alleged benefits conferred. Plaintiffs allege they purchased certain Samsung

[23] *See* Appendix 5 at Column D for cases listing elements of unjust enrichment.

devices (likely from a third-party retailer, although Plaintiffs do not specify)—Samsung phones, watches, headphones, and other electronic products—and received exactly that. (*See, e.g.*, Am. Compl. ¶¶ 33, 36.) When purchasing these devices, data security and protection were "merely incident" to Plaintiffs' purchases. *Irwin*, 175 F. Supp. 3d at 1072. Nor have they alleged that there was anything defective with their products. Courts routinely dismiss unjust enrichment claims in precisely these circumstances. *See, e.g.*, *id.*; *In re Brinker*, 2020 WL 691848 at *11 (same); *In re SuperValu*, 925 F.3d at 966 ("Because [Plaintiff] does not allege that any specific portion of his payment went toward data protection, he has not alleged a benefit conferred in exchange for protection of his personal information nor has he shown how SuperValu's retention of his payment would be inequitable."); *Perdue v. Hy-Vee, Inc.*, 455 F. Supp. 3d at 766 (dismissing unjust enrichment claim because "Plaintiffs have not alleged that any specific portion of their payments went toward data protection . . . Plaintiffs here do not allege that the food or gas they received was defective."); *Gordon v. Chipotle Mexican Grill, Inc.*, 344 F. Supp. 3d 1231, 1249 (D. Colo. 2018) ("Plaintiffs paid for burritos; Plaintiffs received burritos. Plaintiffs' unjust enrichment claim fails to state a claim for which relief may be granted.").

### F. Plaintiffs' Declaratory Judgment Cause of Action Fails

Plaintiffs' declaratory judgment claim in Count 7 should be dismissed because it is not a standalone cause of action, but rather a remedy. The Declaratory Judgment Act does not "create a cause of action" but is merely a "procedural vehicle that creates a form of relief." *In re AZEK Bldg. Prod., Inc., Mktg. & Sales Pracs. Litig.*, 82 F. Supp. 3d 608, 624-25 (D.N.J. 2015). Although Plaintiffs do not specifically plead their claim under the Declaratory Judgment Act, federal law applies in determining "whether and to what extent declaratory relief is warranted." *See W.R. Huff Asset Mgmt. Co. v. William Soroka 1989 Tr.*, 2009 WL 606152, at *2 (D.N.J. Mar. 9, 2009), *amended on other grounds*, 2009 WL 2436692 (D.N.J. Aug. 6, 2009). "[C]ourts within the Third Circuit routinely dismiss stand-alone counts for declaratory and injunctive relief, since such claims are requests for remedies, and not independent causes of action." *Asah v. N.J. Dep't of Educ.*, 330 F. Supp. 3d 975, 1019 n.25 (D.N.J. 2018). Plaintiffs' declaratory judgment claim should be dismissed for this reason alone.

Additionally, Plaintiffs' declaratory judgment claim should be dismissed as wholly duplicative of Plaintiffs' other claims seeking forward-looking relief and adds "nothing to this case" (to the extent any of the claims survive). *In re AZEK*, 82 F. Supp. 3d at 624-25; *see also Mazzoccoli v. Merit Mountainside LLC*, 2012

WL 6697439, at *9 (D.N.J. Dec. 20, 2012). Because Plaintiffs' declaratory judgment claim serves no "useful purpose," it must be dismissed. *Nitta Casings Inc. v. Sompo Japan Ins. Co.*, 2015 WL 7195248, at *2 (D.N.J. Nov. 16, 2015); *see also, e.g.*, *Watkins v. Bai Brands, LLC*, 2018 WL 999677, at *4 (D.N.J. Feb. 20, 2018) (dismissing claim duplicative of breach of contract claim).

## VIII. PLAINTIFFS' STATUTORY CONSUMER FRAUD CLAIMS FAIL

Plaintiffs assert claims under 40 statutory consumer fraud statutes. These claims fail for several reasons. As discussed in Section A, the vast majority of these claims fail for basic and threshold reasons, such as (1) the statute does not include a private right of action for consumers (Section VIII.A.1); (2) the statute prohibits or limits class actions requiring dismissal (Section VIII.A.2); (3) the statutes require pre-suit notice, which Plaintiffs utterly failed to provide (Section VIII.A.3); (4) the statute is limited to injunctive relief and Plaintiffs have failed to allege a need for that relief (Section VIII.A.4); and (5) Plaintiffs' allegations are so deficient that they fail to provide fair notice under Rule 8 of their claims, thus preventing Samsung from even responding (Section VIII.A.5).

As addressed in Section B, Plaintiffs have failed to adequately plead the prima facie elements of consumer fraud. All the consumer fraud statutes sound in fraud. This means that Plaintiffs have to plead their claims with particularity under

Rule 9, which Plaintiffs universally fail to do (Section VIII.B.1). Plaintiffs also fail to plead the other required prima facie elements of their consumer fraud claims, such as reliance (Section VIII.B.2), proximate cause (Section VIII.B.3), and pecuniary injury (Section VIII.B.4). Plaintiff's statutory consumer fraud claims also fail for other state-specific reasons (Sections VIII.B.5-6).

A comprehensive summary of the arguments to dismiss Plaintiffs' consumer fraud claims is attached hereto as Appendix 6.

### A. Plaintiffs' Consumer Fraud Claims Fail for Multiple Threshold Reasons

#### *1. The Ohio Deceptive Practices statute does not contain a private right of action*

"Individual consumers are barred from bringing actions under the" Ohio Deceptive Practices Act. *Michelson v. Volkswagen Aktiengesellschaft*, 99 N.E.3d 475, 479 (Ohio Ct. App. 2018); *see Holbrook v. La.-Pacific Corp.*, 533 Fed. App'x 493, 497-98 (6th Cir. 2013) (affirming dismissal of ODTPA claim because plaintiff lacked "standing to raise an ODTPA claim as a consumer"); *In re MCG Health Data Sec. Issue Litig.*, 2023 WL 3057428, at *10 (W.D. Wash. Mar. 27, 2023), *report and recommendation adopted*, 2023 WL 4131746 (W.D. Wash. June 22, 2023) ("Plaintiffs do not have standing to pursue a claim under the Ohio DTPA"). Accordingly, Plaintiffs' Ohio Deceptive Trade Practices Act claim (Count 48)

must be dismissed.

*2. Certain consumer fraud statutes prohibit or limit class actions*

Plaintiffs may not pursue a class action under the consumer fraud statutes of eight states identified in the Complaint.[24] Multiple courts have dismissed class claims like the Plaintiffs' because the statutes at issue do not permit private class actions. *See, e.g.*, *In re Mednax*, 603 F. Supp. 3d at 1217 ("Plaintiffs assert that Defendants . . . violated the South Carolina Unfair Trade Practices Act . . . Unfortunately for Plaintiffs, this statute expressly prohibits the pursuit of class action claims. So the class claims of Plaintiffs [] must be dismissed.") (citation and quotation marks omitted).

To bring a class action under the Ohio Consumer Sales Practices Act, Plaintiffs must plead that Samsung's specific actions were previously declared deceptive by an administrative rule "adopted under division (B)(2) of section 1345.05" or an Ohio state court decision. Oh. Rev. Code § 1345.09(B) (West). Plaintiffs' citation to the FTC Act (15 U.S.C. § 45) does not suffice because it is neither an administrative rule nor an Ohio state court decision.

[24] These states include Alabama, Arkansas, Georgia, Iowa, Louisiana, Ohio, South Carolina, and Tennessee. The relevant law and named plaintiffs associated with each state are in Appendix 7.

*3. Plaintiffs did not provide pre-suit notice*

Plaintiffs' claims under six state consumer fraud statutes fail because Plaintiffs failed to provide the requisite pre-suit notice of their claims.[25] In conclusory fashion and without any supporting allegations, Plaintiffs allege vaguely that they have "substantially complied" with the notice requirements under the applicable statutes they claim were violated. (*See, e.g.*, Am. Compl. ¶¶ 416-18) (California Consumer Privacy Act). Plaintiffs further allege that "Samsung received written notice of the factual bases of this cause of action and others when plaintiffs in multiple actions that were filed in multiple jurisdictions served Samsung with complaints in connection with the Data Breach. Plaintiffs' attempts to plead pre-suit notice fails.

First, notice that follows, or is contemporaneous with, the filing of a lawsuit is insufficient to satisfy a ***pre***-suit notice requirement. *See, e.g., Beck v. FCA US LLC*, 273 F. Supp. 3d 735, 748 (E.D. Mich. 2017) (stating that "attempt to provide a notice ***after*** filing suit is insufficient to satisfy the CLRA notice requirement"); *Griffey*, 2022 WL 1811165, at *6 (dismissing California Consumer Privacy Act claim with prejudice because "[i]f a notice filed before the 30-day deadline could

[25] These states include Alabama, California, Georgia, Indiana, Massachusetts, and Texas. The relevant law and named plaintiffs associated with each state are in Appendix 8.

be updated when an amended complaint is filed and satisfy the 30-day notice requirement, then having the pre-suit notice requirement would be pointless"). Service of a lawsuit cannot satisfy pre-suit notice requirements. *Outboard Marine Corp. v. Superior Ct.*, 124 Cal. Rptr. 852, 858-59 (Cal. Ct. App. 1975).

Second, MDL consolidation does not change, or excuse the failure to satisfy, the statutory pre-suit notice requirements. *See, e.g.*, *In re Ambry Genetics Data Breach Litig.*, 567 F. Supp. 3d 1130, 1149 (C.D. Cal. 2021) (rejecting argument that "Defendants have long had notice of Plaintiffs' allegations, claims and demands, including from the filing of numerous underlying actions against it arising from the Data Breach, the first of which were filed on or about April 22, 2020"); *In re New Motor Vehicles Canadian Exp. Antitrust Litig.*, 350 F. Supp. 2d 160, 188-89 (D. Me. 2004) ("[T]he initial complaints filed across the country and the Amended Complaint filed in this Court . . . cannot 'effectively act as the required notice.'"). Plaintiffs' allegation that the underlying lawsuits consolidated in this MDL provided Samsung with pre-suit notice is contrary to law. *Id*.

Third, Plaintiffs cannot point to paragraphs 420-21 for their alleged compliance with pre-suit notice in Massachusetts and Texas, as these paragraphs merely set forth the scope of the California Consumer Records Act. To the extent that this is a citation error improperly referring to the original consolidated

complaint, purported compliance "with California Civil Code, Section 1798.150's written notice requirement" does not satisfy their pre-filing notice requirements under the Massachusetts Consumer Protection Act and Texas Deceptive Trade Practices-Consumer Protection Act. (*See* Am. Compl. ¶ 662 ("As set forth in paragraphs 420-421 above, Plaintiff has substantially complied with the notice requirements of Mass. Gen. Laws Ann. Ch. 93A, §9(3)."); *id.* ¶ 944 (As set forth in paragraphs 420-421 above, Plaintiff has substantially complied with the notice requirements of Tex. Bus. & Com. Code § 17.505."). Plaintiffs fail to satisfy other pre-suit notice requirements of the California Consumer Privacy Act ("CCPA"), including attaching the notice to the Complaint. *In re Cap. One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 422 n.30 (E.D. Va. 2020) (dismissing CCPA claims where "Plaintiffs did not attach the required pre-suit notices to the Amended Complaint"). In any event, Plaintiffs' purported partial compliance with the pre-suit notice requirements of the CCPA does nothing to meet their burden of satisfying different statutory requirements of different states.

Finally, Plaintiffs do not allege ***anything*** with respect to the pre-suit notice requirements of the Alabama Deceptive Trade Practices Act, Georgia Fair Business Practices Act, and Indiana Deceptive Consumer Sales Act. This complete failure to plead pre-suit notice is fatal to these claims.

Accordingly, Plaintiffs' claims under the Alabama Deceptive Trade Practices Act (Count 8), California Consumer Privacy Act (Count 13), California Consumer Legal Remedies Act (Count 16), Georgia Fair Business Practices Act (Count 21), Indiana Deceptive Consumer Sales Act (Count 26), Massachusetts Consumer Protection Act (Count 33), and Texas Deceptive Trade Practices-Consumer Protection Act (Count 58) must be dismissed. Simply put, filing a lawsuit is not ***pre***-suit notice.

*4. Certain claims fail because they are limited to injunctive relief*

Plaintiffs cannot pursue consumer fraud claims under the Georgia Uniform Deceptive Practices Act (Count 22), Illinois Uniform Deceptive Trade Practices Act (Count 25), and Minnesota Uniform Deceptive Trade Practices Act (Count 37), which permit only injunctive relief.[26] "Because injunctions regulate future conduct, a party has standing to seek injunctive relief only if the party alleges, and ultimately proves, a real and immediate—as opposed to a merely conjectural or hypothetical—threat of future injury." *Wooden v. Bd. of Regents of Univ. Sys. of Ga.*, 247 F.3d 1262, 1284 (11th Cir. 2001). As explained in Section VI.B.7 *supra*, Plaintiffs have not (and cannot) allege a real and immediate threat of future injury, and thus Plaintiffs' cannot bring consumer fraud claims limited to injunctive relief.

[26] The relevant law and plaintiffs associated with each state are in Appendix 9.

*5. Plaintiffs did not provide fair notice under Rule 8*

Many consumer fraud statutes nominally permit multiple types of claims like deceptive, unfair, and unconscionable claims. But for certain counts, Plaintiffs do not even purport to plead what kind of claim they are asserting. (*See* Am. Compl. ¶¶ 443, 446 (noting that the CLRA "protect[s] consumers against unfair and deceptive business practices" but pleading only that Samsung's "acts and practices were intended to and did result in . . . violation of Civil Code § 1770"); *id*. ¶ 844 ("Samsung engaged in unfair methods of competition and unfair or deceptive acts or practices"); *id.* ¶ 960 ("Samsung engaged in unfair or deceptive acts or practices"). As a result, Samsung is left guessing the legal basis of Plaintiffs' claims. That is not fair notice. *Bardwil Indus. Inc. v. Kennedy*, 2020 WL 2748248, at *4 (S.D.N.Y. May 27, 2020) (dismissing claim because "[s]uch guesswork is antithetical to the 'fair notice' that Rule 8 requires"). This Court should therefore dismiss Counts 16, 51, and 60.

Other counts plead multiple violations but fail to make clear which alleged conduct corresponds to which type of violation. (*See, e.g.*, Am. Compl. ¶ 376 ("Samsung's unfair and deceptive acts and practices included"); *id.* ¶ 540 ("unfair, unlawful, and deceptive trade practices, misrepresentations, and the concealment, suppression, and omission of material facts"); *id.* ¶ 399 (Samsung "engaged in the

following deceptive and unconscionable trade practices"); *id.* ¶ 437 ("Samsung's unlawful, unfair, and deceptive acts and practices include"); *id.* ¶ 492 ("Samsung engaged in unconscionable, unfair, deceptive acts and practices"); *id.* ¶ 563 ("Samsung engaged in unfair, abusive, and deceptive acts, omissions, and practices). But "unfair," "unconscionable," "unlawful," and deceptive" are separate theories of harm with distinct legal requirements under each state law.

For example, Plaintiffs claim that "Samsung engaged in unconscionable, unfair, and deceptive acts and practices" in support of their Florida Deceptive and Unfair Trade Practices Act claim, but nowhere do they include any factual support to explain which of their stock list of three failures, two misrepresentations, and two omissions apply to "unfair" practices as opposed to "deceptive" practices. *Id.* ¶ 492. "[T]he standard for proving the existence of a deceptive act is different than the standard for proving an unfair practice." *Sol. Z v. Alma Lasers, Inc.*, 2013 WL 12246356, at *5 (S.D. Fla. Jan. 22, 2013). A deceptive act is one "likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment." *Kurimski v. Shell Oil Co.*, 570 F. Supp. 3d 1228, 1242 (S.D. Fla. 2021) (citations omitted). By contrast, "an unfair practice is one that offends established public policy or is immoral, unethical, oppressive, unscrupulous or substantially injurious to consumers." *In re Sony*, 996 F. Supp. 2d at 995 (citation and

quotation marks omitted). Simply put, there is no factual content or any explanation of what conduct is allegedly "deceptive" as opposed to "fraudulent," "unfair," "unconscionable," or "unlawful." Courts have dismissed claims, and in many instances, entire "shotgun" pleadings where, as here, "[i]t is virtually impossible to ascertain what factual allegations correspond with each claim." *See, e.g., Beckwith v. Bellsouth Telecomms, Inc.*, 146 F. App'x 368, 372 (11th Cir. 2005). This Court should do the same and dismiss Counts 10-12, 15, 20, 24, 26, 27, 29, 31-33, 35, 36, 41, 43, 46, 47, 52, 55, and 57.

Plaintiffs cannot take shelter under alternative pleading because each alternate theory of liability is equally conclusory. *See, e.g., CAO Grp., Inc. v. Sybron Dental Specialties, Inc.*, 2014 WL 119134, at *3 (D. Utah Jan. 10, 2014) ("While pleading in the alternative under Rule 8(d)(2) is well-recognized and accepted, pleading alternative causes of action does not relieve [Plaintiff of] its obligation to include sufficient factual matter in its complaint in order to comply with the pleading requirements of Rule 8(a)(2) and the 'plausibility' standard set forth in *Iqbal* and *Twombly*."). Plaintiffs employ a check-the-box approach to the consumer fraud statutes that define and enumerate specific acts merely parroting the statutory text, and/or provide the same stock set of seven allegations, including three purported failures, two misrepresentations, and two omissions. *See, e.g., In*

*re Premera Blue Cross*, 198 F. Supp. 3d at 1187-88 ("To be entitled to a presumption of truth, allegations in a complaint 'may not simply recite the elements of a cause of action, but must contain sufficient allegations of underlying facts to give fair notice and to enable the opposing party to defend itself effectively.'").

Where Plaintiffs assert a single cause of action, again the Complaint parrots the statutorily defined practices and/or includes the same stock list of seven conclusory allegations which fail the plausibility standard of Rule 8. *See Iqbal*, 556 U.S. at 663. The Court should dismiss Counts 8 (deceptive), 18 (deceptive), 22 (deceptive), 25 (deceptive), 37 (deceptive), 38 (deceptive), 39 (deceptive), 42 (unconscionable), 44 (deceptive), 48 (deceptive), 49 (unlawful), 50 (unlawful), 58 (deceptive), and 61 (deceptive).

### B. Plaintiffs Fail to Adequately Plead the Prima Facie Elements of Consumer Fraud

Plaintiffs have failed to adequately allege any deceptive conduct or actionable misrepresentation or omission, which, as explained below, are required to plead a violation of the consumer fraud statutes. Even if Plaintiffs were to point to an actionable statement or omission (they have not), Plaintiffs' statutory claims fail because they do not plead the other prima facie elements of a fraud claim: actual reliance, proximate causation, and actual injury.

*1. Plaintiffs fail to plead their consumer fraud claims with particularity as required by Rule 9(b).*

Thirty-six consumer fraud acts cited in the Complaint require Plaintiffs' allegations to meet Rule 9(b)'s heightened pleading standard to plead their consumer fraud claims with particularity. *See* Appendix 10. To withstand a motion to dismiss under Rule 9(b), the Third Circuit "requires, at a minimum, that plaintiffs support their allegations . . . [with] the who, what, when, where and how" of the alleged fraudulent misrepresentation or omission. *In re Suprema Specialties, Inc. Sec. Litig.*, 438 F.3d 256, 276 (3d Cir. 2006) (quotation marks omitted). This includes "the date, time and place of the alleged fraud" or some other "measure[able] substantiation." *Frederico v. Home Depot*, 507 F.3d 188, 200 (3d Cir. 2007). These heightened pleading requirements "serv[] important objectives" of giving "defendants notice of the claims against them, provid[ing] an increased measure of protection for their reputations, and reduc[ing] the number of frivolous suits brought solely to extract settlements." *Rockefeller Ctr. Props., Inc. Sec. Litig.*, 311 F.3d 198, 216 (3d Cir. 2002). Plaintiffs' allegations of deceptive conduct, misrepresentations, and omissions falls well short of this exacting standard.

a. Plaintiffs' recitations of alleged failures is not sufficient to establish their claims based on deceptive, fraudulent, unfair, unconscionable, or unlawful conduct

Plaintiffs allege the following failures: (1) "Failing to implement and maintain reasonable security and privacy measures to protect Subclass Members' PII, which was a direct and proximate cause of the Data Breach;" (2) "Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;" and (3) "Failing to comply with common law and statutory duties pertaining to the security and privacy of Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach." (*See, e.g.*, Am. Compl. ¶ 376 (a)-(c).)

The Complaint includes no ***factual contentions*** as to ***how*** the three alleged failures identified were deceptive—if that is Plaintiffs' theory. Samsung is left "guessing as to the what, when, where, and how of the misconduct alleged." *James Erickson Fam. P'ship LLLP v. Transamerica Life Ins. Co.*, 2019 WL 1755858, at *4 (D. Ariz. Apr. 19, 2019). Courts routinely dismiss conclusory claims under consumer fraud statutes for lack of "supporting factual contentions." *Franklin v. Apple*, 569 F. Supp. 3d 465, 480-81 (E.D. Tex. 2021); *accord Doe v.*

*CVS Pharmacy*, 982 F.3d 1204, 1214-15 (9th Cir. 2020) (dismissing UCL unfairness claims where "complaint left the district court to guess what conduct Plaintiffs alleged satisfied the 'unfair' prong of the UCL"); *Fuccillo v. Century Enters., Inc.*, 2019 WL 11648480, at *7 (M.D. Fla. Mar. 8, 2019) (dismissing FDUTPA unfairness claim with prejudice because "Plaintiffs have done no more than recite the elements of this claim, without any supporting facts"); *HW Aviation LLC v. Royal Sons, LLC*, 2008 WL 4327296, at *6 (M.D. Fla. Sept. 17, 2008) (collecting cases and dismissing FDUTPA claim because it did "not specify what conduct was allegedly deceptive, unfair, or unconscionable"). Merely pointing to alleged failures (1) does not demonstrate deceptive, fraudulent, unfair, unconscionable, or unlawful conduct; and (2) does not nudge Plaintiffs' claims across the plausibility threshold.

b. Plaintiffs do not plausibly allege any misrepresentations

Plaintiffs allege the following misrepresentations: (1) "Misrepresenting that it would protect the privacy and confidentiality of Subclass Members' PII, including by implementing and maintaining reasonable security measures;" and (2) "Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45." (*See, e.g.*, Am. Compl. ¶ 376(d), (e).)

Purportedly to demonstrate misrepresentations, Plaintiffs cite the following excerpts cherry-picked from Samsung's online privacy and security policies: "[W]e prioritize protecting your information;" "We take data security very seriously. Our products are designed to keep your data private and secure . . . ;" Samsung devices and services are "designed with privacy and security at top of mind;" "We are committed to protecting your privacy . . . ;" "At Samsung Mobile, security and privacy are at the core of what we do and what we think about every day;" Samsung has "industry-leading security;" and Samsung takes "a holistic approach to security to ensure that, at all levels of the device, we are protecting users' security and privacy at all times." (Am. Compl. ¶ 197.) Plaintiffs' citation to these provisions demonstrates both their confusion and the lack of factual substance underlying their labels and conclusions couched as allegations of fact. While these statements relate to ***product*** *or* ***device*** security, there is no allegation that the Security Incident involved a breach of any products or devices.

With respect to the first alleged misrepresentation regarding "protect[ing] the privacy and confidentiality" of Plaintiffs' PII (*see, e.g.*, Am. Compl. ¶ 356(d)), these sorts of vague, aspirational, and generalized statements cannot state a consumer fraud claim. *See, e.g.*, *In re Am. Med. Collection Agency, Inc. Customer Data Sec. Breach Litig.*, 2021 WL 5937742, at *25 (D.N.J. Dec. 16, 2021)

(Defendant's "vow to take 'great care' to protect Personal Information is not an actionable representation. Indeed, it is unclear that this assertion can be considered a statement of objective fact, as opposed to mere puffery"); *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, 2017 WL 3727318, at *26 (N.D. Cal. Aug. 30, 2017) (holding that statement in privacy policy that "protecting . . . our users' information is paramount" was non-actionable puffery) (quotation marks omitted). No reasonable consumer would read the statement as a guarantee that Samsung would not be the victim of a cyber-attack that would compromise PII. *See Abdale v. N. Shore Long Island Jewish Health Sys.*, 19 N.Y.S.3d 850, 859-60 (N.Y. Sup. Ct. 2015) ("[P]rivacy policy and online notices do not constitute an unlimited guaranty that patient information could not be stolen" and "did not mislead the plaintiffs in any material way.").

More importantly, there is "no workable standard by which to assess the falsity of Defendants' privacy and data security statements, nor have plaintiffs provided the Court with one. [Plaintiff] has therefore failed to allege an actionable misrepresentation." *In re Am. Med. Collection Agency*, 2021 WL 5937742, at *25-26. Plaintiffs merely point to promises about data security and allege such promises were a misrepresentation based on the fact a data breach occurred. Without more, this kind of *ipse dixit* allegation does not sustain a consumer

protection claim. *See, e.g.*, *Griffey*, 562 F. Supp. 3d at 55 (Plaintiff's "Wisconsin claim fails because he has not explained with any specificity how [Defendant's] data security was inadequate beyond pointing to the fact that a security breach happened. That is a conclusory allegation. Rivera fails to state a Wisconsin DTPA claim").

So too for the second alleged misrepresentation regarding compliance with "statutory and common law duties" pertaining to data security. Courts have applied Rule 9(b) and dismissed state consumer fraud claims where, as here, the alleged misrepresentation is not a statement of objective fact but instead a legal conclusion couched as an allegation of fact. *See, e.g.*, *In re: Am. Fin. Res., Inc. Data Breach Litig.*, 2023 WL 3963804, at *11 (D.N.J. Mar. 29, 2023) (Plaintiff "further alleges that '[Defendant] engaged in these acts or omissions by failing to comply with common law and statutory requirements for adequate data security.' These are conclusory statements that fail to provide the 'the time, place, and contents of the false representations' as required."); *Anderson v. Kimpton Hotel & Rest. Grp., LLC*, 2019 WL 3753308, at *7 (N.D. Cal. Aug. 8, 2019) (applying Rule 9(b) and dismissing claim because "the complaint includes no facts, as opposed to conclusions, to support a finding that any misrepresentation or omission was false, let alone false at the time made").

Accordingly, to the extent their consumer fraud claims are based on purported misrepresentations, the claims must be dismissed. *See* Appendix 11.

c. Plaintiffs do not plausibly allege actionable omissions

Plaintiffs' consumer fraud claims appear to be based, in part, on purported omissions. Plaintiffs claim that Samsung violated the consumer fraud statutes by "[o]mitting, suppressing, and concealing" two "material" facts: (1) "that it did not properly secure . . . Subclass Members' PII;" and (2) "that it did not comply with common law and statutory duties pertaining to the security and privacy of . . . Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45." (*See, e.g.*, Am. Compl. ¶ 376(f), (g).) These alleged "material omissions" are not actionable for at least three reasons.

First, 11 consumer fraud statutes cited in the Complaint require that the defendant ***knowingly*** committed the fraudulent omissions. *See* Appendix 12. Here, Plaintiffs do not plead any factual allegations demonstrating Samsung knew of any security deficiency ***at the time of the Security Incident***. Merely pointing to the fact that the incident occurred, or that there may have been past incidents, does not demonstrate that Samsung had actual knowledge that its data security practices were inadequate at the time of ***this*** incident (which they were not).

Second, 27 of the consumer fraud laws require a Plaintiff to show that the

defendant had a duty to disclose the allegedly omitted information. *See* Appendix 12. In the absence of a confidential relationship, no duty to disclose exists when parties are engaged in arm's-length business negotiations; in fact, an arm's-length relationship by its nature excludes a confidential relationship." *In re Equifax*, 362 F. Supp. 3d at 1337 (citations and quotations omitted)). Plaintiffs do not even allege they engaged in an arm's-length retail transaction with Samsung—they merely allege that they "purchased" Samsung products or services from some unknown entity. (*See, e.g.*, Am. Compl. ¶ 33 (stating that a named plaintiff "purchased" a Samsung phone)); *see also, e.g.*, *In re Equifax, Inc.*, 362 F. Supp. 3d at 1337. And Plaintiffs do not allege a "confidential relationship" giving rise to a duty to disclose. *See Huynh v. Quora, Inc.*, 2020 WL 7408230, at *12 (N.D. Cal. June 1, 2020).

Third, these alleged omissions are not actionable as pled. With respect to the first alleged omission that Samsung did not did not properly secure its customers' PII, courts have "typically require[d] the claimant to plead the type of facts omitted, the place in which the omissions should have appeared, and the way in which the omitted facts made the representations misleading." *Carroll v. Fort James Corp.*, 470 F.3d 1171, 1174 (5th Cir. 2006). Failing to allege these

particularized details warrants dismissal. *See In re VTech Data Breach Litig.*, 2018 WL 1863953, at *7 (N.D. Ill. Apr. 18, 2018).

As for the second alleged omission that Samsung "did not comply with common law and statutory duties pertaining to the security and privacy" of PII (Am. Compl. ¶ 376(g)), courts have rejected substantially similar allegations as a non-actionable legal conclusion. *In re Am. Med. Collection Agency, Inc.*, 2021 WL 5937742, at *26.

*2. Plaintiffs fail to plead reliance*

Twenty-three consumer fraud statutes require plaintiffs to show actual reliance on alleged misrepresentations or omissions resulting in harm. *See* Appendix 13. Here, even if Plaintiffs were able to point to an affirmative misrepresentation or material omission (they have not), they fail to adequately allege reliance upon the policies and statements they cite.[27] Plaintiffs allege that

[27] *See, e.g., In re Solara Med. Supplies, LLC Customer Data Sec. Breach Litig.*, 613 F. Supp. 3d 1284, 1302 (S.D. Cal. 2020) ("Plaintiffs fail to adequately plead their misrepresentation claim to the extent they rely on statements in the Privacy Policy for Solara's software application and the Terms and Service of their website. Plaintiffs do not allege having been exposed to the statements in either the software application or Solara's website."); *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, 2017 WL 3727318, at *30 (N.D. Cal. Aug. 30, 2017) ("Plaintiffs do not allege that they actually read Defendants' Privacy Policy. Accordingly . . . Plaintiffs have not alleged that, had Defendants disclosed in their Privacy Policy that Defendants' security systems were non-compliant and substandard, Plaintiffs would have been aware of this disclosure." (quotation

(Footnote Cont'd on Following Page)

"Plaintiffs and other Class Members relied to their detriment on Samsung's numerous false representations regarding data security" (Am. Compl. ¶ 199), but include zero facts that any class member actually saw—much less read and relied upon—any of Samsung's policies or statements contained therein prior to their purchases from unknown retailers. Because Plaintiffs fail to allege any facts with specificity showing that they saw and actually relied upon the policies and statements cited, the Court should dismiss the 23 claims listed in Appendix 13.

*3. Plaintiffs fail to plead proximate causation*

Twenty-nine consumer fraud statutes require Plaintiffs to plead proximate causation. *See* Appendix 14. This requires facts demonstrating that the "alleged unlawful practice[s of Samsung were the] proximate cause of the . . . [Plaintiffs'] ascertainable loss."[28] No Plaintiff plausibly alleges they were exposed to any

---

marks omitted)); *In re Am. Med. Collection Agency, Inc.*, 2021 WL 5937742, at *27, 30 (finding that a "vast majority" of plaintiffs failed to allege reliance because in some instances those "plaintiffs [did] not allege that they read LabCorp's privacy policies.").

[28] *Marcus v. BMW of N. Am., LLC*, 687 F.3d 583, 606 (3d Cir. 2012) (discussing New Jersey Consumer Fraud Act claim); *see also e.g.*, *Gale v. Int'l Bus. Machines Corp.*, 781 N.Y.S.2d 45, 46-47 (N.Y. App. Div. 2004) (affirming dismissal of claim brought under New York's General Business Law where plaintiff failed to allege "that the defendant's material deceptive act caused the injury"); *Antman*, 2015 WL 6123054, at *11 (dismissing California Unfair Competition Law ("UCL") claim where plaintiff "did not allege a causal connection between Uber's conduct and the [alleged injury]").

representation, omission, deceptive act, or unfair practice by Samsung at any point ***before*** the Security Incident. Lacking such allegations, Plaintiffs have not alleged that Samsung proximately caused their supposed injuries, and their consumer protection act claims necessarily fail. *See* Appendix 14 (listing cases).

*4. Plaintiffs fail to plead actual, pecuniary injury*

Thirty-six of the consumer fraud laws under which Plaintiffs assert claims require "ascertainable loss of money or property," "pecuniary loss," "monetary damage," or some other form of actual injury caused by the defendant as a result of an alleged statutory violation. *See* Appendix 15 (listing cases).

Fifteen Plaintiffs do not allege actual, pecuniary harm, but instead allege attempted identity theft/fraud, time spent monitoring for fraud, miscellaneous expenses, and/or lost benefit of the bargain. *See* Appendix 1. None of their theories of injury satisfies the injury requirements. *See* Appendix 15.

Plaintiffs' allegations of "attempted" identity theft/fraud focus on a perceived increase in scam text, emails, and phone calls, or a notification that Plaintiffs' PII was listed on the Dark Web. But a risk of fraud and identity theft does not satisfy state consumer fraud act injury requirements because such speculative allegations are "not sufficient to allege 'lost money or property'" as

many states require.[29] Nor is this "hypothetical" harm sufficiently "quantifiable or measurable" to qualify as "ascertainable loss"[30] or satisfy other states' "actual injury" or damages requirements.[31]

Mitigation efforts are not cognizable as an actual injury for consumer fraud purposes. Plaintiffs wrongly seek to recover for the time they allegedly spent mitigating the purported future risk of harm by reviewing credit statements or

---

[29] *Mueller v. Harry Kaufmann Motorcars, Inc.*, 859 N.W.2d 451, 459 (Wis. Ct. App. 2014) (Wisconsin requires showing of "monetary loss"); *Joseph v. Nordstrom, Inc.*, 2016 WL 6917279, at *3 (C.D. Cal. June 17, 2016) (CLRA requires "economic injury"); *Shaulis v. Nordstrom, Inc.*, 865 F.3d 1, 10 (1st Cir. 2017) (Mass. Ch. 93A requires "real economic damages," not just a "risk").

[30] *Thiedemann v. Mercedes-Benz, USA, LLC*, 872 A.2d 783, 792, 793, 795, 796 (N.J. 2005) (finding no injury under NJCFA's "ascertainable loss" requirement); *see also Holmes v. Countrywide Fin. Corp.*, 2012 WL 2873892, at *11, 14 (W.D. Ky. July 12, 2012) (same under the Kentucky and New Jersey law).

[31] *See Precision Links Inc. v. USA Prod. Grp., Inc.*, 2009 WL 801781, at *3 (W.D.N.C. Mar. 25, 2009) (dismissing NCUDTPA claim based on "speculative allegations of possible harm in the future"); *Hammond*, 2010 WL 2643307, at *12-13 (dismissing New York, California, and New Jersey claims based on "increased risk of identity theft"); *Resnick v. AvMed, Inc.*, 2011 WL 1303217, at *1 (S.D. Fla. Apr. 5, 2011) (same under Florida law); *Attias*, 365 F. Supp. 3d at 13 (same under Maryland law); *Harrison v. Leviton Mfg. Co.*, 2006 WL 2990524, at *4-5 (N.D. Okla. Oct. 19, 2016) (Oklahoma Consumer Protection Act prohibits recovery of damages for actions that "will only hypothetically cause[] [them] harm"); *Gerboc v. ContextLogic, Inc.*, 867 F.3d 675, 680-81 (6th Cir. 2017) (under Ohio Consumer Sales Protection Act "plaintiff must have suffered an injury or loss"); *Stein v. Sprint Corp.*, 22 F. Supp. 2d 1210, 1216 (D. Kan. 1998) (Kansas requires that plaintiff actually "suffered an injury"), *on reconsideration* (Aug. 27, 1998).

(Footnote Cont'd on Following Page)

monitoring their credit (*see, e.g.*, Am. Compl. ¶ 35), while a subset allegedly purchased or otherwise obtained password or credit monitoring services (*id.* ¶ 38), or instituted credit freezes (*id.* ¶ 77). None of these allegations are sufficient. Indeed, "the vast majority of courts . . . in the context of data-breach litigation" have refused to allow recovery for these types of "preventative expenditures" because they are "anticipated" and "not actual damages." *Attias*, 365 F. Supp. 3d at 14-15. Regardless of the applicable injury requirement—whether economic injury or damages,[32] ascertainable loss,[33] actual damages or

[32] *See Shaulis*, 865 F.3d at 1 (must show "economic loss" under Massachusetts consumer protection act); *In re Sony*, 903 F. Supp. 2d at 966 (mitigation measures insufficient under the UCL and CLRA).

[33] *Holmes*, 2012 WL 2873892, at *11, 14 ("time monitoring their credit" and credit monitoring fees not "ascertainable loss[es]" under Kentucky and New Jersey law); *see also Gupta v. Asha Enterprises, L.L.C.*, 27 A.3d 953, 960 (N.J. App. Div. 2011) ("cost of cure" allegations insufficient unless underlying injury is, itself, a "loss of moneys or property").

(Footnote Cont'd on Following Page)

injury,[34] or pecuniary loss,[35]—such allegations of voluntary mitigation measures to guard against speculative, future harm are not sufficient.

Lost benefit of the bargain—that Plaintiffs "would not have purchased the above-mentioned Samsung products or services or would have paid less for them"—is also not a cognizable injury to state a consumer fraud claim. *See supra*, Section VI.B.2.

The remaining 34 Plaintiffs allege some form of actual identity theft or fraud in the form of unauthorized charges or unauthorized credit card inquiries. *See* Appendix 1. But only Plaintiff Steven Baker (whose claims should be dismissed for other reasons, *see* Appendix 15) specifically alleges that the monetary loss remains unremedied or unreimbursed, and thus that he actually lost money as a result of the unauthorized charges. As to the others, there is no "reasonable

[34] *Rollins, Inc. v. Butland*, 951 So.2d 860, 873 (Fla. Dist. Ct. App. 2006) (Florida law "does not provide for the recovery of . . . speculative losses"); *Shafran*, 2008 WL 763177, at *2 (finding "time and money . . . spent to guard against identity theft," including credit monitoring, were not cognizable injuries); *Coker v. Daimler Chrysler Corp.*, 617 S.E.2d 306, 313 (N.C. Ct. App. 2005) (affirming dismissal of NCUDTPA claims for lack of injury where plaintiffs sought damages "for possible future expenses not yet incurred," including "the cost of 'supposed' remedial measures"); *Finstad v. Washburn Univ.*, 845 P.2d. 685, 691 (Kan. 1993).

[35] *See In re SuperValu, Inc.*, 925 F.3d at 964-65 (lost time monitoring credit, a "single fraudulent charge," and "effort expended replacing [that] card" did not qualify as "actual damage" or "pecuniary loss").

[inference]" of any economic loss in such circumstances because "federal law and card-issuer contracts ordinarily absolve the consumer from any obligation to pay the fraudulent charge." *In re SuperValu*, 925 F.3d at 964 (holding that such allegations insufficient to show "actual damages" under consumer acts); *Dugas v. Starwood Hotels & Resorts Worldwide, Inc.*, 2016 WL 6523428, at *4 (S.D. Cal. Nov. 3, 2016) (finding that unauthorized but reimbursed charges did not satisfy as "loss of money or property" under California UCL). Similarly, Plaintiffs have not alleged any out-of-pocket expenses or other loss as a result of the alleged credit card inquiries. *See, e.g.*, *Kimbriel v. ABB, Inc.*, 2019 WL 4861168, at *3 (E.D.N.C. Oct. 1, 2019) (finding that credit inquiries not an injury-in-fact because they did not "plausibly show that plaintiffs' compromised data is being used or that future use . . . is 'certainly impending'").

As a result, Plaintiffs' consumer fraud claims requiring actual injury must be dismissed with the exception of Plaintiff Baker's claim under the Wisconsin Deceptive Trade Practices Act, which fails for other reasons. *See* Appendix 15.

*5. Plaintiffs fail to plead a monetary transaction between Plaintiffs and Defendant*

Thirteen consumer fraud laws require that a plaintiff must have paid money to the defendant directly and not to an intermediary vendor or reseller. *See* Appendix 16; *see also In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 715

(N.D. Cal. 2011), *aff'd*, 572 F. App'x 494 (9th Cir. 2014) (applying California law and noting that only "a plaintiff who is a *consumer* of certain services (i.e., who 'paid fees' for those services) may state a claim"); *Cellco P'ship v. Hope*, 2011 WL 3159172, at *4 (D. Ariz. July 26, 2011) (Arizona Consumer Fraud Act); *Badillo v. Playboy Entm't Grp., Inc*., 2006 WL 785707, at *6 (M.D. Fla. Mar. 28, 2006) (Florida Deceptive and Unfair Trade Practices Act). Here, none of the Plaintiffs specifically allege that he or she personally purchased any product directly from Samsung. They merely allege that they "purchased" Samsung products, but fail to allege they purchased these from products directly from Samsung as opposed to an unspecified retailer. This pleading failure is fatal. This Court should dismiss the 13 claims listed in Appendix 16.

*6. Certain claims fail for independent state-specific reasons*

a. Plaintiffs' consumer fraud claims based upon violations of relevant data breach notification statutes fail

Plaintiffs' theory for their Connecticut Unfair Trade Practices Act claim is an alleged violation of the Breach of Security Regarding Computerized Data Act, C.G.S.A. § 36a-701b. (Am. Compl. ¶ 480.). As explained in Section IX.B *infra*, Plaintiffs have not alleged a cognizable injury resulting from deficient notification, and cannot allege a violation of the notification statute. Since Plaintiffs include no facts other than the alleged violation of the Breach of Security Regarding

Computerized Data, Plaintiffs' derivative claim under the Connecticut Unfair Trade Practices Act (Count 19) must be dismissed.

To the extent Plaintiffs include a violation of relevant data breach notification statutes as a predicate act supporting their consumer fraud claims, those claims fail because there is no violation of any data breach notification statute. *See* Section IX. As a result, the Court should dismiss claims under the Iowa Private Right of Action for Consumer Frauds Act (Count 27), Michigan Consumer Protection Act (Count 35), New Jersey Consumer Fraud Act (Count 42), and the Wisconsin Deceptive Trade Practices Act (Count 61).

b. Plaintiffs' California Unfair Competition Law ("UCL") Claim Fails

i. California Plaintiffs do not adequately plead entitlement to either of the two remedies available under the UCL

"Remedies under the UCL are limited to restitution and injunctive relief, and do not include damages." *In re Ambry Genetics Data Breach Litig.*, 567 F. Supp. 3d at 1147 (citing *Silvercrest Realty, Inc. v. Great Am. E&S Ins. Co.*, 2012 WL 13028094, at *2 (C.D. Cal. Apr. 4, 2012)). Because these are equitable remedies, they are "not available unless the plaintiff lacks an adequate remedy at law." *Id.* Accordingly, a plaintiff must establish that there is no adequate remedy at law before securing an equitable remedy for past harm under the UCL. *See Sonner v.*

*Premier Nutrition Corp.*, 971 F.3d 834, 844 (9th Cir. 2020). But as discussed above, Plaintiffs here cannot plausibly allege that they do not have an adequate remedy at law. *See supra* Section VII.E.2. This alone warrants dismissal of the UCL cause of action.[36] *See id.*; *In re Ambry Genetics Data Breach Litig.*, 567 F. Supp. 3d at 1147.

Moreover, as explained in Section VI.B.7 *supra*, Plaintiffs have not (and cannot) allege a real and immediate threat of future injury. To the extent the Plaintiffs seek injunctive relief under the UCL, this claim fails.

ii. California Plaintiffs fail to allege conduct that satisfies any of the three UCL prongs

California's UCL prohibits "any unlawful, unfair or fraudulent business act or practice." *See* Cal. Civ. Code § 17200. First, to maintain a claim under the "unlawful" prong of the UCL, a Plaintiff must allege facts sufficient to state a claim that Samsung's conduct violated some other borrowed law. *See Klein v. Chevron U.S.A., Inc.*, 137 Cal. Rptr. 3d 293, 326 (Cal. Ct. App. 2012). California Plaintiffs here base their claim under the UCL's unlawful prong on alleged violations of the FTC Act, the California Consumer Records Act ("CRA"), the

[36] To the extent that California Plaintiffs also seek injunctive relief or other equitable remedies under the CLRA, that should also be dismissed for the same reasons. *See Sonner v. Premier Nutrition Corp.*, 971 F.3d at 844; *Philips v. Ford Motor Co.*, 2015 WL 4111448, at *16 (N.D. Cal. July 7, 2015).

California Consumer Legal Remedies Act ("CLRA"), and California common law (Am. Compl. ¶ 436.) Plaintiffs cannot base their UCL claim on a purported violation of the FTC Act because it solely contemplates administrative enforcement, and as such cannot serve as the basis for an "unlawful" UCL claim. *See* 15 U.S.C. § 45; *Zhang v. Superior Ct.*, 304 P.3d 163, 177 (Cal. 2013); *Carlson v. Coca-Cola Co.*, 483 F.2d 279, 280 (9th Cir. 1973) ("The protection against unfair trade practices afforded by the [FTC] Act vests initial remedial power solely in the Federal Trade Commission."). More generally, Plaintiffs' "unlawful" prong claim fails because they have failed to allege facts sufficient to state claims for violations of the FTC Act, CLRA, CRA, or California common law, as discussed both *supra* and *infra*. Because these claims fail, so too must Plaintiffs' claim under the "unlawful" prong of the UCL.

Second, to the extent that California Plaintiffs bring their claim under the "fraudulent" prong of the UCL,[37] this fails for the same reason discussed in Section VIII.B.1 *supra*—Plaintiffs have not pled this claim with particularity under Rule 9(b). *See, e.g.*, *Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1125 (9th Cir. 2009).

[37] While the Complaint does not explicitly state whether California Plaintiffs bring a cause of action pursuant to the "fraudulent" prong of the UCL, Plaintiffs do allege Samsung engaged in "deceptive acts and practices" and "fraudulent acts and practices." (*See, e.g.*, Am. Compl. ¶¶ 437, 439.)

Third, "[a] business practice is unfair within the meaning of the UCL if it violates established public policy or if it is immoral, unethical, oppressive or unscrupulous and causes injury to consumers which outweighs its benefits." *Nolte v. Cedars-Sinai Med. Ctr.*, 187 Cal. Rptr. 3d 737, 743 (Cal. Ct. App. 2015) (citation omitted). California Plaintiffs fail to allege conduct by Samsung that rises to this level of "unfair" practices. They do broadly allege that data was stolen in the Security Incident because Samsung failed to "properly secure" their data. But what they do not do is allege facts that support the conclusion that Samsung's failure to prevent the Security Incident somehow constitutes immoral, unethical, oppressive, or unscrupulous conduct. Plaintiffs' conclusory assertion that "Samsung's failure to implement and maintain reasonable security measures was also contrary legislatively-declared public policy that seeks to protect consumers' data" reflected in the FTC Act, the CRA, and the California Consumer Privacy Act ("CCPA") is insufficient to state a claim under this prong (Am. Compl. ¶ 435(e).) Plaintiffs do not allege facts that demonstrate Samsung's conduct fits these conclusory statements, and the Ninth Circuit has affirmed dismissal of similarly general allegations of unfair conduct. *See Levitt v. Yelp! Inc.*, 765 F.3d 1123, 1136 (9th Cir. 2014). Also, because these statutes cannot serve as the basis for a viable claim under the "unlawful" prong as discussed above, a claim under the "unfair"

prong based on the same statutes and conduct, as it is here, must fail as well. *See Hadley v. Kellogg Sales Co.*, 243 F. Supp. 3d 1074, 1104-05 (N.D. Cal. 2017).

c. Plaintiffs' California CLRA claim fails because there is no transaction alleged between Plaintiffs and Samsung

The CLRA requires that a plaintiff demonstrate they suffered damages resulting from "unfair or deceptive practices . . . undertaken by any person ***in a transaction*** intended to result or that results in the sale or lease of goods or services to any consumer." Cal. Civ. Code § 1770(a) (emphasis added); *see also id.* § 1780(a). A "transaction" is defined as "an agreement between a consumer and another person, whether or not the agreement is a contract enforceable by action, and includes the making of, and the performance pursuant to, that agreement." *Id.* § 1761(e).

Both state and federal courts in California have interpreted this language as requiring that a CLRA plaintiff's injury arise out of a transaction between the plaintiff and the defendant. *See, e.g.*, *Dipito LLC v. Manheim Invs., Inc.*, 2021 WL 5908994, at *15 (S.D. Cal. Dec. 14, 2021) (observing that the plaintiff "could not bring a claim under the CLRA against Defendants because there was no transaction between [Plaintiff] and Defendants"); *Green v. Canidae Corp.*, 2009 WL 9421226, at *4 (C.D. Cal. June 9, 2009) ("The CLRA does not provide a cause

of action for consumers against the supplier of goods and services to a retailer from whom the consumer purchased.").

Here, the California Plaintiffs have not alleged they purchased products directly from Samsung (Am. Compl. ¶¶ 45-56.) Nor have they alleged any other transaction or "agreement" between them and Samsung within the meaning of the CLRA that could form the basis of their CLRA claim. Thus, because the complaint is devoid of any allegations of this requisite "transaction," the CLRA claim must be dismissed.

## IX. PLAINTIFFS' DATA BREACH STATUTORY NOTIFICATION CLAIMS FAIL

Plaintiffs bring claims alleging violations of 12 data breach notification statutes. All of these claims fail for one or more of the following reasons: (1) there is no private right of action (Section IX.1); (2) there is no alleged injury related to delayed notification (Section IX.2); (2) Plaintiffs have failed to allege a violation of any state data breach notification statute (Section IX.3); and (4) Plaintiffs' claims under the California Consumer Privacy Act ("CCPA") and California Consumer Records Act ("CCRA") fail for independent reasons (Section IX.4).

### A. Plaintiffs Cannot Assert Claims Under Data Breach Statutes That Do Not Provide a Private Right of Action

Three of the data breach notification statutes identified in the Complaint do not provide a private right of action. *See* Appendix 17 (Colorado, Illinois, Kansas); *see also In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d at 1338 (dismissing claims under several state data breach notification statutes because they do not create private rights of action).

### B. Plaintiffs Do Not Plausibly Allege an Injury from Delayed or Deficient Notification

Nine of the statutes require that Plaintiffs allege actual injury damages that resulted from the alleged delay or deficiency in notification—separate and apart from any injury alleged from the data breach itself. *See* Appendix 18; *see also In re Sony*, 996 F. Supp. 2d at 1010 ("Plaintiff must allege actual damages flowing from the unreasonable delay (and not just the intrusion itself) in order to recover actual damages."); *Grigsby v. Valve Corp.*, 2013 WL 12310666, at *5 (W.D. Wash. Mar. 18, 2013) (Plaintiff must "allege facts supporting the claim that he was injured due to the interval between the hacking incident and [defendant's] notice of the incident and not just that he was injured by the hacking incident alone."); *In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d at 1217-18 (finding that "Plaintiffs [ha[d] not alleged any injury traceable to Adobe's alleged failure to reasonably

notify customers of the . . . data breach).

Plaintiffs have not done that here. Instead, Plaintiffs simply assert that "[a]s a direct and proximate result of Samsung's violations" of the breach notification statutes, Plaintiffs "suffered damages," as described elsewhere in the Complaint. (*See, e.g.*, Am. Compl. ¶ 371.) Plaintiffs include zero facts establishing a causal nexus between their alleged damages and the purportedly delayed notification (as distinct from damages flowing from the data breach itself). That is fatal to their claims. *Antman v. Uber Techs., Inc.*, 2015 WL 6123054, at *11 (N.D. Cal. Oct. 19, 2015) (plaintiff "did not plead injury related to the delay; delay alone is not enough"); *Corona v. Sony Pictures Entm't, Inc.*, 2015 WL 3916744, *8-9 (C.D. Cal. June 15, 2015) (dismissing claims under data breach notification statutes for failure to allege injury resulting from delay).

### C. Plaintiffs Have Failed to Allege a Violation of Any State Data Breach Notification Statute

Plaintiffs cannot state a claim for violation of the data breach notification statutes because Samsung was not legally obligated to notify outside North Dakota and Washington. Despite Plaintiffs' unfounded and unsupportable allegations, Samsung's Notice—which is incorporated by reference into the Complaint—explicitly stated that Social Security numbers and credit card numbers were ***not*** involved in the incident. Other than in North Dakota and Washington, which

require notification where a date of birth is included, there is no requirement to notify based on the data elements involved in the incident.

Regardless, Samsung provided timely notice as a matter of law. Plaintiffs allege that on August 4, 2022, Samsung discovered that an unauthorized third party exfiltrated certain data of its valued customers in July 2022. In less than a month, Samsung undertook a comprehensive and diligent investigation of the Security Incident and provided notification to potentially affected customers. Plaintiffs allege no ***facts*** suggesting Samsung knew or should have known about the Security Incident earlier than it did, or that once Samsung learned of the intrusion, it unreasonably delayed notification. Several data-breach-notification statutes relied on by Plaintiffs permit an entity that has suffered a breach to determine the scope of the breach before notifying consumers. *See, e.g.*, Cal. Civ. Code § 1798.82(a) (delay permitted when "consistent with . . . any measures necessary to determine the scope of the breach"); N.Y. Gen. Bus. Law § 899-a(2) (same). Additionally, several data breach notification statutes set outside time limits on what is reasonable, ***none of which*** is shorter than 30 days. *See, e.g.*, Colo. Rev. Stat. § 6-1-71; Fla. Stat. § 501.171; Wash. Rev. Code § 19.255.010 et seq. Accordingly, Samsung provided timely notice satisfying even the most restrictive state data breach notification laws. Plaintiffs allege that the notification was "untimely" but

provide no specific factual allegations in support of this conclusion, and therefore fail to state a claim under any of the data breach statutes.

The content of Samsung's Notice was also sufficient as a matter of law. Plaintiffs have not, and cannot, plausibly allege that the content of the Notice fails to satisfy any specific data breach notification statute. Plaintiffs allege that "[b]y failing to disclose the Data Breach in a timely and accurate manner, Samsung violated" the various breach notification statutes, but Plaintiffs do not cite or allege any specific inaccuracy, instead merely griping that the notice was "carefully worded" and "unconscionably vague and self-serving." (Am. Compl. ¶¶ 213-14.) The only information Plaintiffs claim was left out was "how many customers' PII was breached," which type of customers—business or consumer, for example—were impacted," and "a breakdown of affected regions." (*Id.* ¶¶ 215, 217.) But, Plaintiffs' only support for this being required in a legal notification is an online article from TechCrunch—not any legal authority or breach notification statute. (*Id.* ¶ 217.) Plaintiffs fail to explain why an individual receiving notice would need to know the number of other people or whether they were a business or consumer customer. And Plaintiffs' claim that the Notice did not satisfy the "formatting requirements" of the CCPA and did not notify the California Attorney

General (*id.* ¶ 222.) is of no moment, since as described above, Samsung had no legal duty to notify under that statute.

Accordingly, this Court should dismiss Counts 9, 13, 14, 17, 23, 28, 30, 40, 45, 54, 56, and 59.

### D. Plaintiffs' CCPA and CRA (§ 1798.81.5) Claims Independently Fail Because Plaintiffs' Conclusory Allegations Regarding Samsung's Security Protocols Are Insufficient

"To state a CCPA claim, a plaintiff must allege that his or her PII was accessed 'as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.'" *Maag v. U.S. Bank, Nat'l Ass'n*, 2021 WL 5605278, at *2 (S.D. Cal. Apr. 8, 2021) (quoting Cal. Civ. Code § 1798.150(a)(1)). The requirements to state a claim under the CRA are nearly identical. *See* Cal. Civ. Code § 1798.81.5(b); *Anderson v. Kimpton Hotel & Rest. Grp., LLC*, 2019 WL 3753308, at *5 (N.D. Cal. Aug. 8, 2019). But merely asserting that a defendant's security measures are lacking is insufficient—a plaintiff must allege "facts to support the notion that the Defendant's security was deficient." *Maag*, 2021 WL 5605278, at *2 (CCPA); *see also Anderson*, 2019 WL 3753308, at *5 (CRA).

Here, the Complaint is devoid of any factual allegations explaining why Samsung's security was deficient or unreasonable. Plaintiffs cite a Forbes article

(like TechCrunch, not a legal authority) where "[d]ata security experts" have apparently stated that most data breaches are preventable if widely-available advice is followed, but do not explain what specific "widely-available advice" Samsung failed to follow in this instance. (Am. Compl. ¶ 255.) Plaintiffs also generally assert that Samsung should have encrypted "the sensitive data elements within the PII it collected" (*id.* ¶ 254), but the allegation that it did not appears to be based purely "upon information and belief" (*id.* ¶ 10), and Plaintiffs fail to explain the basis for it or why this would be unreasonable or not in keeping with industry standards. *See Razuki v. Caliber Home Loans, Inc.*, 2018 WL 6018361, at *2 (S.D. Cal. Nov. 15, 2018) (dismissing CRA claim when plaintiff did not plead the facts that led "him to believe [defendant] didn't comply with industry standards" or what other companies were doing that defendant was not). In short, Plaintiffs' assertion that Samsung's data maintenance practices were unreasonable is conclusory and unsupported by factual allegations. Instead, it appears Plaintiffs have "simply recited a few buzz words with the hope that [they] may be able to figure out later what, if anything, [Samsung] has done wrong." *Id.* Such generalized allegations are insufficient to state claims under the CCPA and CRA, and as such these claims should be dismissed.

## X. PLAINTIFFS' STATUTORY CLAIMS FOR INVASION OF PRIVACY FAIL

### A. The Rhode Island Right to Privacy Claim Fails

Plaintiffs assert violation of Rhode Island's Right to Privacy Statute, which protects the rights to be secure from (1) "unreasonable intrusion upon one's physical solitude or seclusion;" (2) "an appropriation of one's name or likeness;" (3) "unreasonable publicity given to one's private life;" and (4) "publicity that reasonably places another in a false light before the public." *Liu v. Striuli*, 36 F. Supp. 2d 452, 479 (D.R.I. 1999). To recover, "it must be established that: (A) [there] was an invasion of something that is entitled to be private or would be expected to be private; and (B) the invasion was or is offensive or objectionable to a reasonable man." *Laccinole v. Students for Life Action Inc.*, 2022 WL 3099211, at *6 (D.R.I. Aug. 4, 2022) (quoting R.I. Gen. Laws § 9-1-28.1(a)(1)). Confusingly, Plaintiffs' allegations merge and conflate two distinct strains of privacy violations under the statute. (Am. Compl. ¶ 869 ("Samsung intentionally intruded into Plaintiff's and Rhode Island Subclass Members' seclusion by disclosing without permission their PII to a third party.")).

Samsung is aware of no case applying this statute to an alleged data breach. This is for good reason: to the extent Plaintiffs are alleging an intrusion upon seclusion claim based on the Security Incident, the information must have been acquired through "wrongful or improper means" and the disclosure must be

intentional. *Pontbriand v. Sundlun*, 699 A.2d 856, 863 (R.I. 1997). Here, Plaintiffs allege no facts that Samsung wrongfully or improperly acquired Plaintiffs' PII and plead no facts that Samsung intentionally disclosed this information when it was the unexpected victim of the instant Security Incident.[38] Therefore, Plaintiffs' novel theory fails, and Plaintiffs' claim for Right to Privacy (Count 53) must be dismissed.

### B. The Massachusetts Privacy Statute Claim Fails

Plaintiffs also allege a violation of Massachusetts Privacy Statute. Massachusetts law recognizes "a right against unreasonable, substantial or serious interference with [a person's] privacy." Mass. Gen. Laws ch. 214, § 1B. To state a claim under this statute, an interference with privacy must be both "unreasonable" and "serious or substantial." *Schlesinger v. Merrill Lynch, Pierce, Fenner & Smith, Inc.*, 567 N.E.2d 912, 914 (Mass. 1991). It also requires an ***intentional*** disclosure of "facts of a private nature" made without any "legitimate, countervailing interest for the disclosure." *See Barrigas v. United States*, 2018 WL 1244780, at *7 (D. Mass. Mar. 9, 2018) (quotation marks and citations omitted);

[38] In fact, Plaintiffs voluntarily dropped their invasion of privacy common law claims.

Mass. Gen. Laws ch. 258, § 10 (listing "invasion of privacy" as an "intentional tort"); *Nelson v. Salem State College*, 845 N.E.2d 338, 348 (Mass. 2006) (same).

Here, Plaintiffs cannot plausibly allege that Samsung intentionally invaded Plaintiffs' privacy. According to the Complaint, Samsung was the victim of a third party criminal's cyber-attack. (Am. Compl. ¶ 211.) Thus, even if Plaintiffs had alleged information has been disclosed to an unauthorized third-party, Plaintiffs cannot and have not alleged that Samsung disclosed the PII intentionally, as required to violate the Massachusetts Privacy Statute. *Barrigas*, 2018 WL 1244780, at *7. Accordingly, Plaintiffs' claim for violation of the Massachusetts Privacy Statute (Count 34) must be dismissed.

## CONCLUSION

For the foregoing reasons, Samsung respectfully requests that the Court dismiss Plaintiffs' Complaint in its entirety with prejudice.

Dated: August 11, 2023

Respectfully submitted,

**ARCHER & GREINER, P.C.**

By: */s/ Carlos M. Bollar*
Carlos M. Bollar
Maureen Coghlan
1025 Laurel Oak Road

Voorhees, NJ 08043
Tel: (856) 795-2121
Fax: (856) 795-0574
cbollar@archerlaw.com
mcoghlan@archerlaw.com

**HUNTON ANDREWS KURTH LLP**

By: */s/ Neil K. Gilman*

Neil K. Gilman
Michael J. Mueller
2200 Pennsylvania Ave. NW
Washington, DC 20009
Tel: (202) 955-1500
Fax: (202) 778-2201
ngilman@HuntonAK.com
mmueller@HuntonAK.com

**ARNOLD & PORTER KAYE SCHOLER LLP**

By: */s/ Arthur E. Brown*

Arthur E. Brown
Elie Salamon
250 West 55th Street
New York, NY 10019
Tel: (212) 836-8000
Fax: (212) 836-8689
arthur.brown@arnoldporter.com
elie.salamon@arnoldporter.com

Daniel E. Raymond
70 West Madison Street

Suite 4200
Chicago, IL 60602
daniel.raymond@arnoldporter.com

*Attorneys for Defendant Samsung Electronics America, Inc.*

227602451 v1